OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

FOCUS ON INTERNET SEARCHES FOR EU LEGAL PRACTITIONERS

Vilnius, 14-15 June 2022

UP GRADE
YOUR LEGAL EXPERTISE

Criminal Law

Speakers

Steven David Brown, International Cybercrime Consultant, Vienna

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

Federico Donelli, Lawyer, Avvocati Bonati-Delsignore-Fiaccadori, Parma; PhD, University of Teramo

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

Joachim Meese, Professor, Criminal Law and Procedure, University of Antwerp; Attorney, Bar of Ghent

Aleksandra Stępniewska, Counsel, Polish Law Office WKB (Wierciński, Kwieciński, Baehr), Warsaw

Mindaugas Taškūnas, Prosecutor, Regional Prosecutor's Office, Vilnius

Marc van der Ham, Senior Legal Advisor, High Tech Crime Unit, National Office of the Dutch Public Prosecution Service, PHD Candidate, eLaw – Centre for Law and Digital Technologies, University of Leiden

Saulius Verseckas, Deputy Prosecutor General, Prosecutor General's Office, Vilnius

George Zlati, Attorney, Cluj Bar; PhD on Cybercrime, Babeș Bolyai University, Cluj-Napoca

Key topics

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

Language
English

Event number
322DT04f

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

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

Tuesday, 14 June 2022

08:30 Arrival and registration of participants

09:00 **Welcome and introduction to the programme**
Saulius Verseckas & Laviero Buono

I. TECHNICAL ISSUES AND BASIC UNDERSTANDING OF INTERNET ARCHITECTURE AND CONCEPTS

Chair: Laviero Buono

09:15 **Internet searches and computer forensics in criminal cases: using open source intelligence to gather evidence online**
- OSINT and SOCMINT: a silver bullet for searching for evidence?
- Search engines: how do they work?
- Alternative search engines to explore the hidden Internet
- Main obstacles getting data from online sources or "How to think as a hacker?"
- Visualisation of forensics findings – must or nice-to-have

Rūta Jašinskienė

10:15 Discussion

10:30 Break

11:00 **Who do you think they are?**
- Fake personas & sock puppets
- The danger in deep fakes
- Locating witnesses & suspects
- Ways around encryption

Steven David Brown

12:15 Discussion

12:30 Lunch

II. LEGAL ISSUES RELATED TO INTERNET SEARCHES

Chair: Steven David Brown

14:00 **Search and seizure of stored computer data: technical and legal aspects**
- ECHR jurisprudence
- Computer systems and computer-data storage mediums
- Plain view vs. exploratory search
- The relevance of volatile and non-volatile digital evidence
- The dark side of timestamps
- Thumbcache and child sexual abuse material

George Zlati

14:45 **The collection of evidence located abroad and the challenges of transborder access to data**
- Search across jurisdictions / devices seized
- Transborder access to data
- Cloud computing
- European enforcement challenges in the online context
- Shortcomings and remedies

Federico Donelli

15:30 Discussion

16:00 Break

Objective

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

About the project

This seminar is part of a large-scale project sponsored by the European Commission entitled "Obtaining e-evidence when investigating and prosecuting crimes". It consists of six seminars to take place in Dublin, Thessaloniki, Prague, Trier, Cracow and Vilnius.

Who should attend?

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

Location

Lithuanian Prosecutor General's Office
Rinktines Str. 5A
01515 Vilnius

CPD

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

Your contact persons

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

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

Chair: Laviero Buono

16:30 **The (limited) effectiveness of MLA instruments in the digital age**
- Legal framework and problems regarding traditional MLA in the digital age
- European enforcement challenges in the online context
- Specificities and challenges of criminal cases where anonymous networks and encrypted files are involved

Joachim Meese

17:15 Discussion

17:30 End of first day

20:00 Dinner offered by the organisers

Wednesday, 15 June 2022

III. PRESENTING INTERNET SEARCHES AND E-EVIDENCE IN COURT: PROSECUTION AND DEFENCE PERSPECTIVES (BEST PRACTICES)

Chair: Joachim Meese

09:30 **Internet search results and e-evidence in court: a new evidentiary frontier for prosecutors**
- Challenges posed by websites and social networks
- Proving the authenticity of the data
- Ensuring that the data has not been altered
- Proof of intent
- Presentation of evidence in court

Marc van der Ham

10:15 **Handling electronic evidence in courts: the defence perspective**
- Capturing evidence from the internet: open source and covert
- The importance of the chain of custody in handling the evidence
- Trial considerations: methods of presentation and admissibility tests

Aleksandra Stępniewska

11:00 Discussion

11:15 Break

Chair: Laviero Buono

11:45 **Online investigations and the e-evidence chain of custody through sample cases**
- Establishment of the chain of custody
- Forensic copies
- Hash function: use and limitation

Mindaugas Taškūnas

12:30 Discussion

12:45 End of seminar and lunch

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

Apply online for this seminar:
www.era.int/?131085&en

Save the date

Understanding Bitcoins and Cryptocurrency Technologies
Trier/Online, 25-26 April 2022

Artificial Intelligence in Criminal Justice
Warsaw, 19-20 May 2022

www.era.int/elearning

This programme has been produced with the financial support of the Justice Programme 2014-2020 of the European Union.

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

Application

Obtaining e-evidence when investigating and prosecuting crimes

Vilnius, 15-16 June 2022 / Event number: 322DT04f

Terms and conditions of participation

Selection

1. Participation is only open to judges, prosecutors and lawyers in private practice from eligible EU Member States.
2. 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 (CEJ) must apply for this event through CEJ.
3. Applications should be submitted before **9 May 2022.**
4. 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

5. €225 including documentation, lunches and dinner.

Travel expenses

6. Travel costs up to €300 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

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

Other services

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

Participation

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

Apply online for "**Obtaining e-evidence when investigating and prosecuting crimes**": www.era.int/?131085&en

Location
Lithuanian Prosecutor General's Office
Rinktines Str. 5A
01515 Vilnius

Language
English

Contact Person
Susanne Babion
Assistant
sbabion@era.int
+49 651 9 37 37 - 422

NRD Cyber Security

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

Rūta Jašinskienė
Information analysis expert, NRD Cyber Security

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

NRD Cyber Security

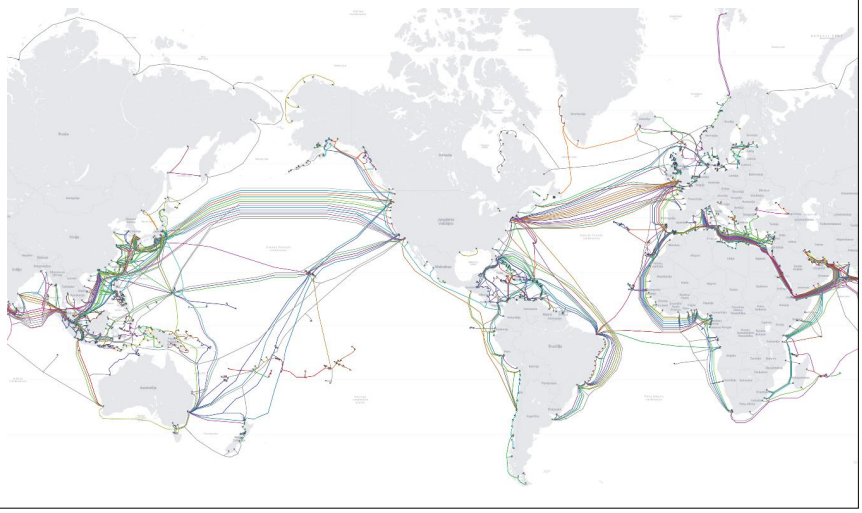
Introduction

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

NRD Cyber Security

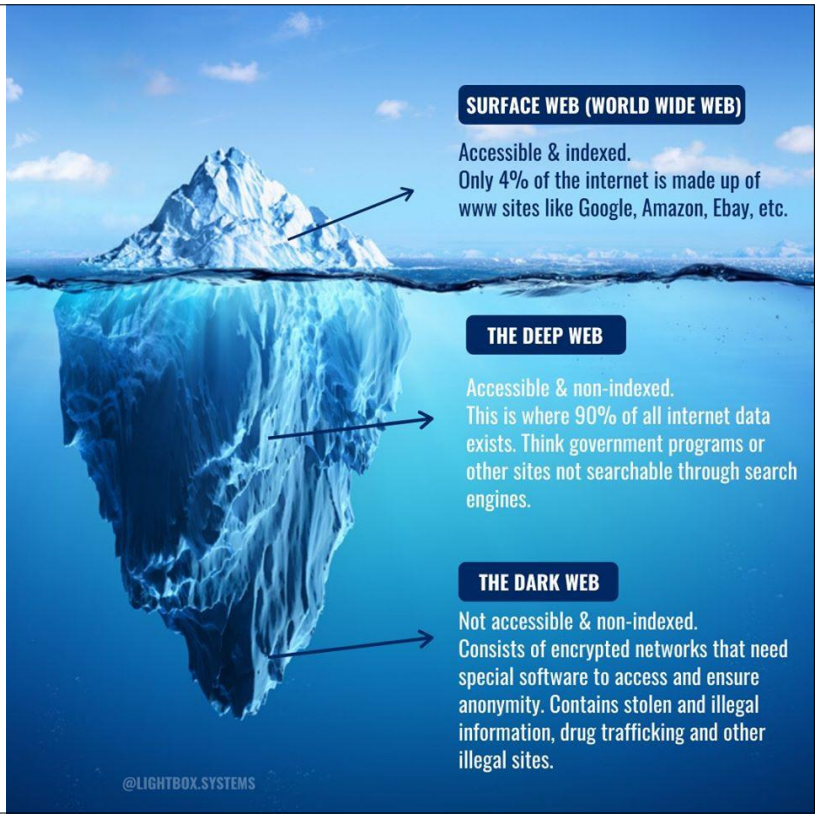
Definitions

The Internet is the global system of interconnected computer networks that uses the Internet protocols to communicate between networks and devices.



NRD Cyber Security

Definitions



NRD Cyber Security

Which option is correct?

1) Data = Information = Intelligence

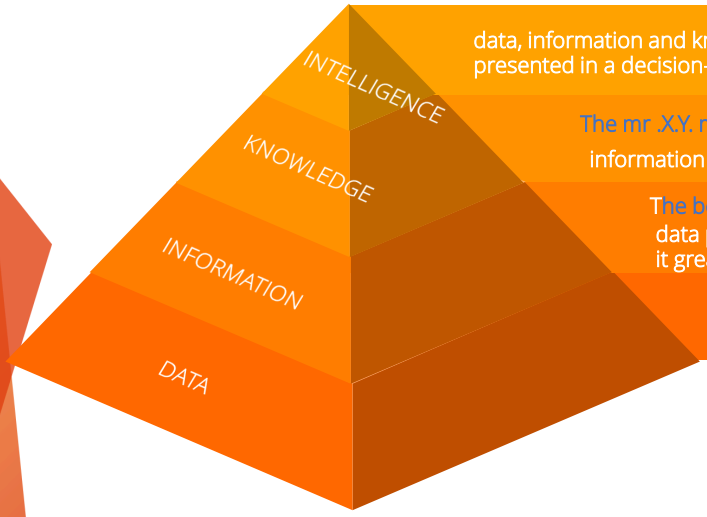
2) Data ≠ Information = Intelligence

3) Data = Information ≠ Intelligence

4) Data ≠ Information ≠ Intelligence

NRD Cyber Security

Knowledge Pyramid,



data, information and knowledge that have been evaluated, analysed and presented in a decision-making format for action-oriented purposes

The mr .X.Y. member of Parliament was robbed and murdered

information that has been given an interpretation and understanding

The body was found on a street in Kaunas last Friday

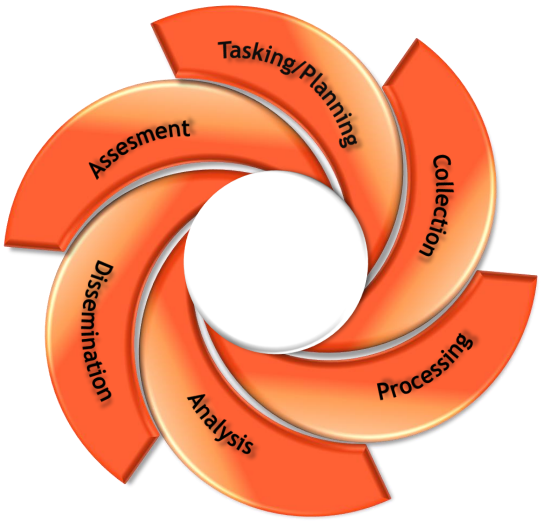
data put in context and empowered with meaning, which gives it greater relevance and purpose

41 24.2028, 210.4418 25.03.2022

raw and uninterpreted observations and measurements

INTELLIGENCE

DON'T JUMP TO CONCLUSIONS – TAKE THE RIGHT STEPS!



NRD Cyber Security

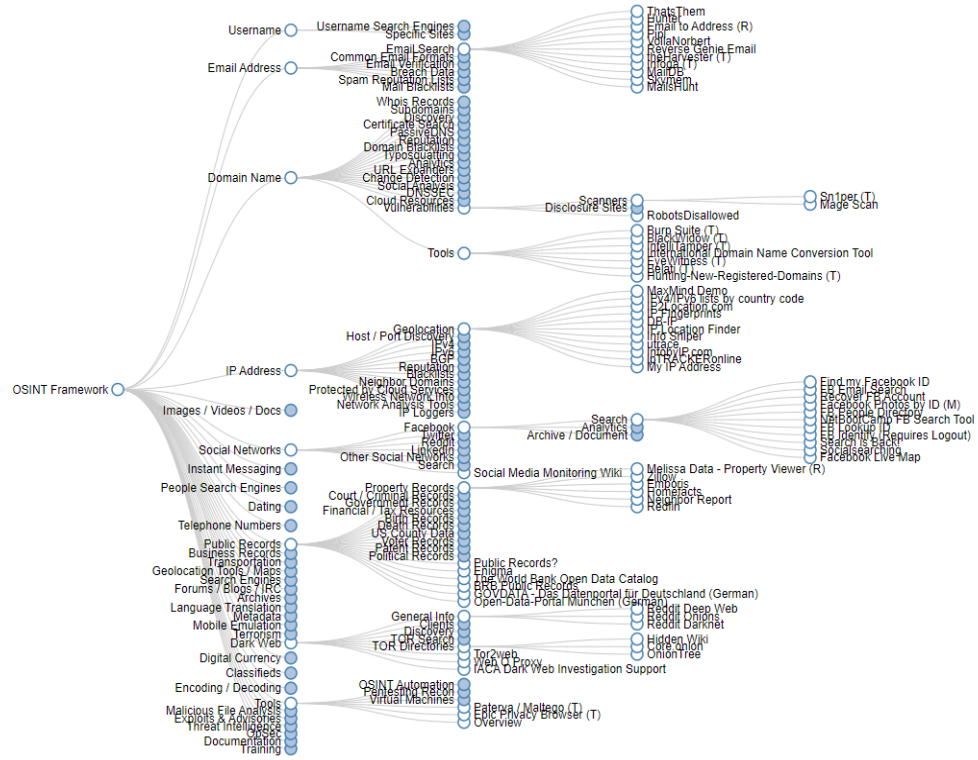
OPEN-SOURCE INTELLIGENCE (OSINT)

- OSINT is intelligence derived from publicly available sources of information. Such information can be:

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

NRD Cyber Security

OSINT Framework

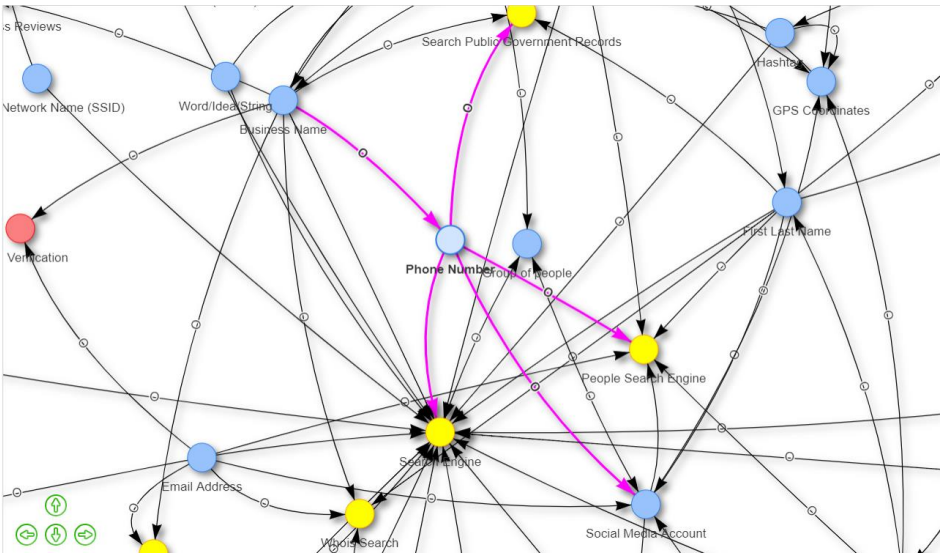


https://osintframework.con

NRD Cyber Security

YOGA

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



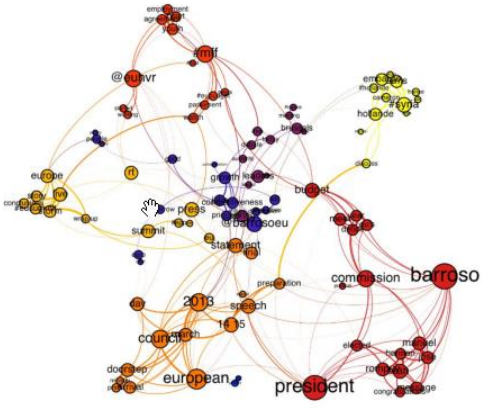
https://yoga.osint.ninja/

What OSINT is Not?

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

Social Media Intelligence (SOCMINT)

- SOCMINT is intelligence derived from information and data gathered from social media sources
- Such information can be public or private.
- It consists in gathering information about anything based on what is publicly available on social media, like pictures, location data, or simply content



NRD Cyber Security

Types of social media platforms

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

NRD Cyber Security

OSINT benefits

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

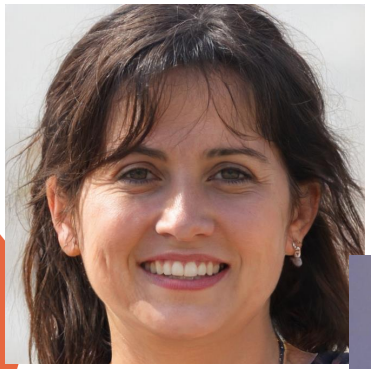
NRD Cyber Security

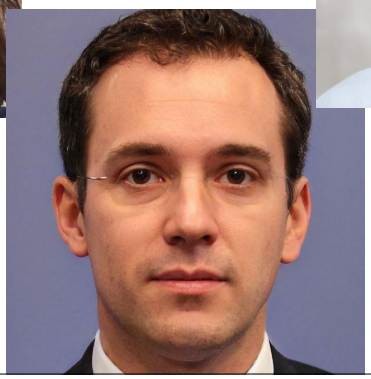
Why OSINT does NOT a silver bullet?

- Overwhelming
- Reliability
- Validity
- Inadequate training and investment

NRD Cyber Security

Who of these people doesn't exist?





NRD Cyber Security

Source reliability and information validity

anna holligan
@annaholligan

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

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

2:30 AM · Jun 6, 2019

3 10 Copy link to Tweet

Lisa Westerveld
@Lisawesterveld

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

euronews.

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

By Lauren Chadwick 04/06/2019

INDEPENDENT

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

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

HEARTBREAKING

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

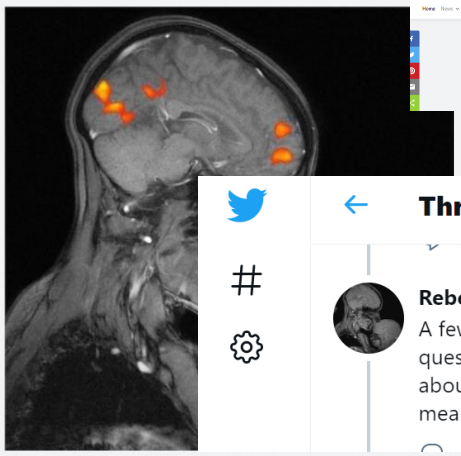
Daily Mail MORE STORIES

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

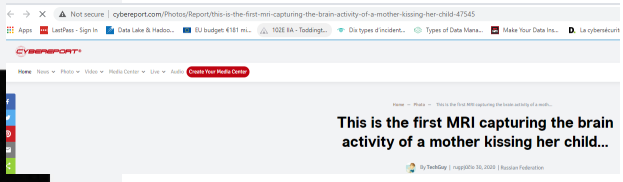
NRD Cyber Security

This is the first MRI capturing the brain activity of a mother kissing her child...

By TechGuy | rugpjūčio 30, 2020 | Russian Federation



Her kiss has caused a chemical reaction in her baby's brain. Source Credit : @rebecca_saxe , @MIT

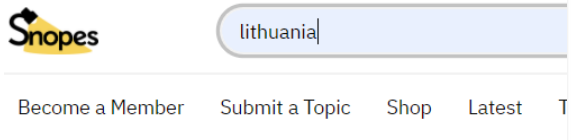


Thread

Rebecca Saxe @rebecca_saxe · 12 Sep 2019

A few years ago, I was doing an fMRI study of infant brains. The scientific questions we were asking (with amazing grad student @bmhdeen) were about the organization of functional activity in infant brains when viewing meaningful visual images, like faces and natural scenes.

Fake news?



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

Search Engines

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

NRD Cyber Security

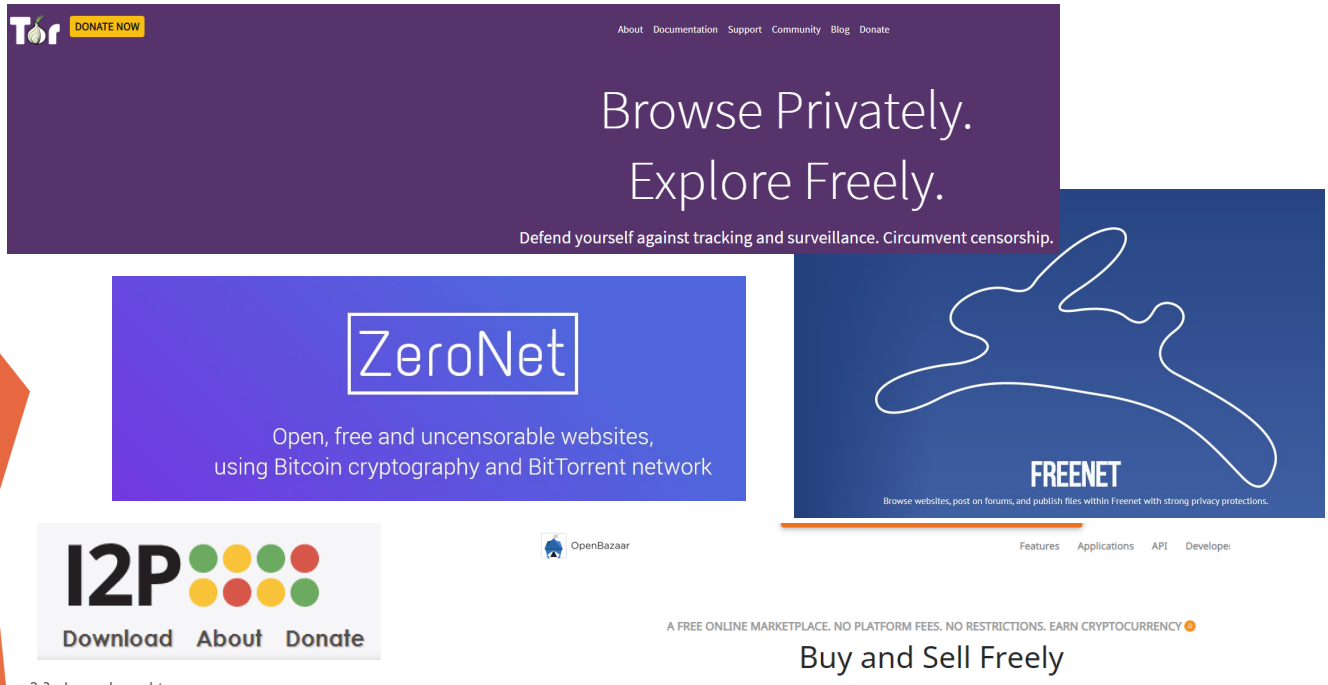
Popular General Search Engines

- Google
- Bing
- Yahoo
- Yandex
- Baidu
- DuckDuckGo
- ...

NRD Cyber Security

Specialized Search Engines

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



Tor Network

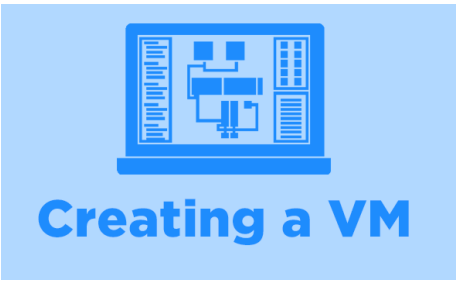
- Onion Services are the most anonymous web servers that exist today
- **IP addresses are not used** for Onion Services – no possibility to scan every IP address on the planet, like we can do for the WWW
- It is not possible to connect IP addresses to domain names, like we can do on the WWW
- You need to know the URL of the website you are going to visit
- Most dark marketplaces have some human readability into their URLs at least
  - e.g. http://**cannazon**ceujdye3.onion/
  - e.g. http://**garden**2b7zwrjskh2y3f4pkscgg2waogjp2ilax2mvikjlzmamylznad.onion
  - e.g. http://**ciadotgov**4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/index.html
  - e.g. **facebook**wkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion

TOR network

- Over 2 million users access the Tor platform daily.
- Only 45% of websites on the dark web host illicit activities.
- Tor hosts over 65,000 unique URLs with the .onion extension.
- Russia has the biggest share of daily Tor users.
- Bitcoin transactions on the dark web were on track to reach $1 billion in 2019.

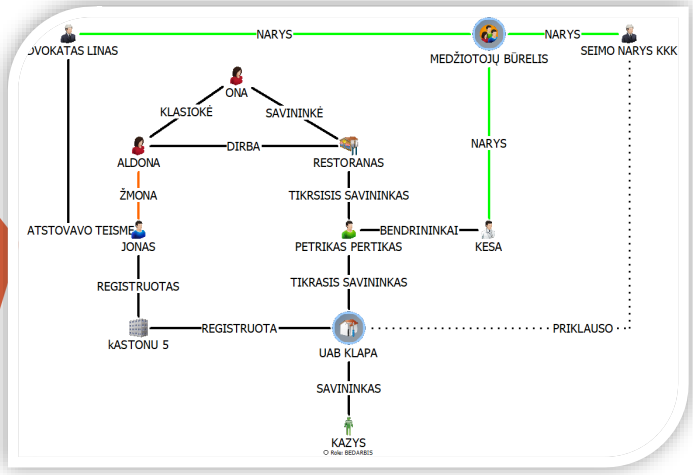
Do not leave a footprint behind….

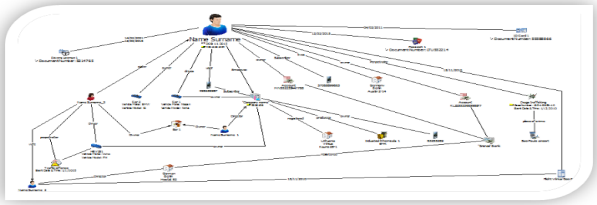
- https://randomuser.me/
- https://www.name-generator.org.uk/
- https://www.fakenamegenerator.com/
- https://this-person-does-not-exist.com/en

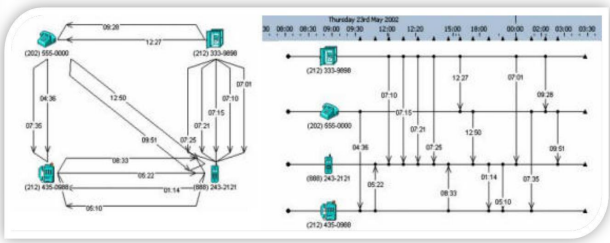


NRD Cyber Security

One image replaces a thousand words

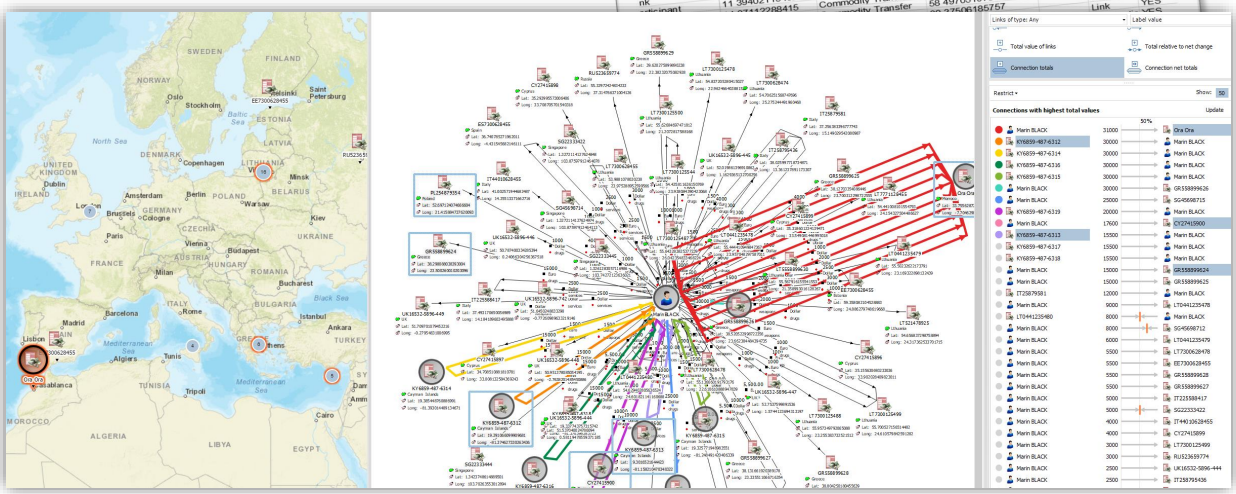






NRD Cyber Security

Perception



Thank you!!!!

Rūta JAŠINSKIENĖ

rj@nrdcs.lt

www.linkedin.com/in/ruta-jasinskiene

"On the Internet nobody knows you're a dog …"

InZeit
Excellence in Acuity

Cat Photo by Unknown Author is licensed under CC BY-NC

Sockpuppets

InZeit
Excellence in Acuity

sock puppet

[sok-puhp-it]

noun

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

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

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

InZeit
Excellence in Acuity

Create Social Media accounts

Mask ID

Who? Why?

Criminal

Other Investigators (e.g. journalists)

Law Enforcement

Protect ID from revenge attack

Not to flag investigation underway

InZeit Excellence in Acuity

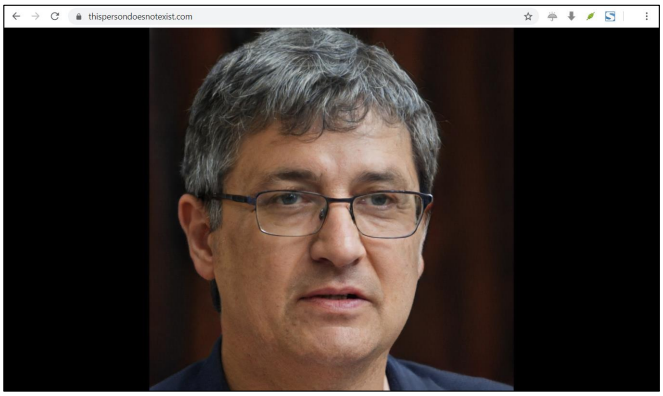
How?

InZeit Excellence in Acuity

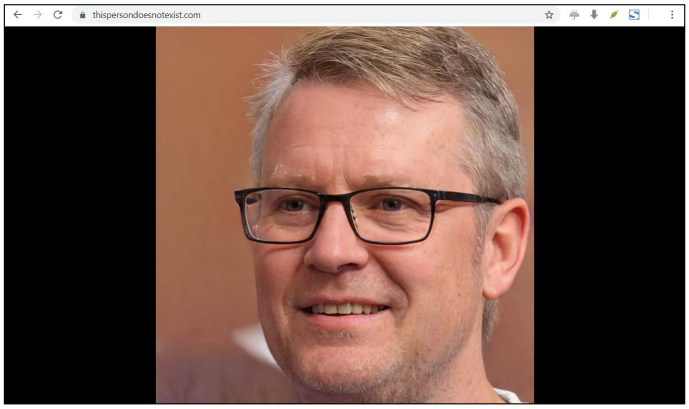
First, make a face …

InZeit
Excellence in Acuity

InZeit
Excellence in Acuity



thispersondoesnotexist.com



InZeit
Excellence in Acuity

Creating Online Presence (online accounts):

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

Many require mobile phone number

May require backup email for validation

May require SMS validation

InZeit
Excellence in Acuity

Creating Online Presence (online accounts):
Also want to 'hide' IP Address BUT:
Most well known email providers block VPNs (and VPN providers may have logs)

Solution:

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

InZeit
Excellence in Acuity

Public wifi access points risks:

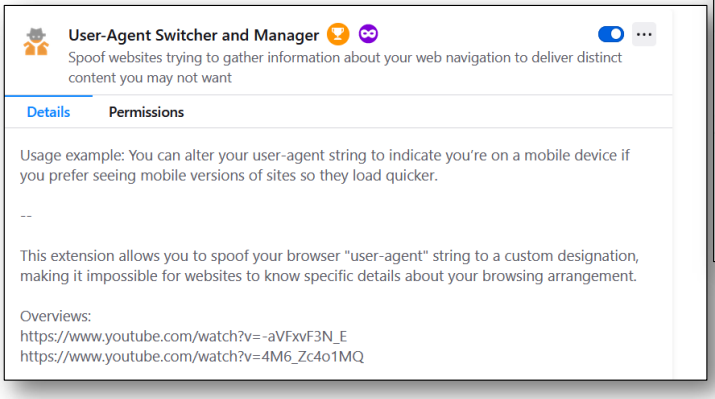
Fake access point
(Man-In-The-Middle)

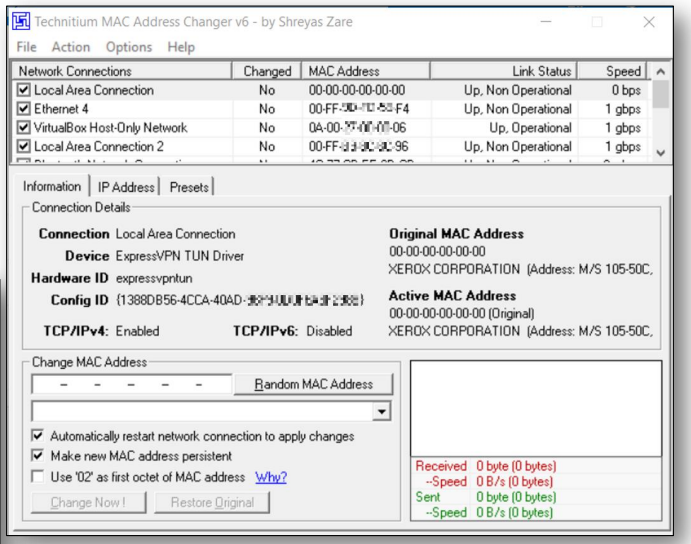
Your MAC/IMEI address is logged by network
Use MAC Changer app.

Browser fingerprinting
Use 'clean' browser
Remove add-ons/extensions
Delete cookies/history
Use a User-Agent Manager/Switcher

InZeit
Excellence in Acuity

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





MAC Changer App.

InZeit Excellence in Acuity

Creating Online Presence (online accounts):

Many require mobile phone number

Solution:

Get a burner phone
(not so easy – more later)

InZeit Excellence in Acuity

Creating Online Presence (online accounts):

Some providers require backup email for validation

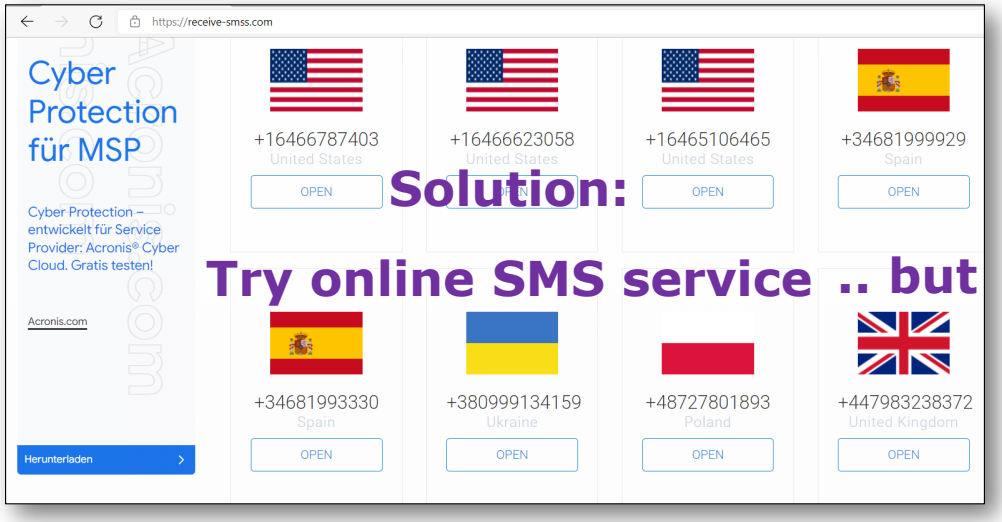
Solution:

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

InZeit Excellence in Acuity

Creating Online Presence (online accounts):

Some require SMS validation



Solution:

Try online SMS service .. but

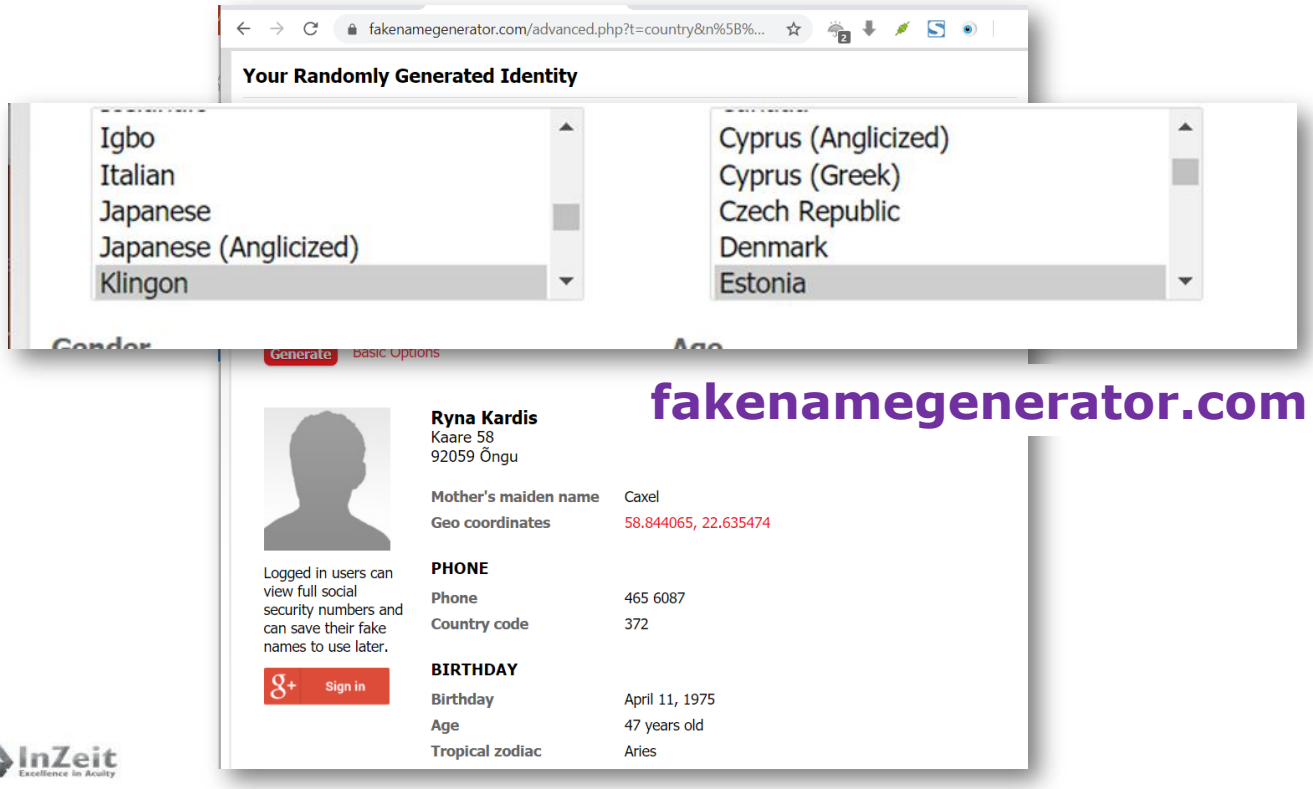
InZeit Excellence in Acuity

https://receive-smss.com/

Build character profile

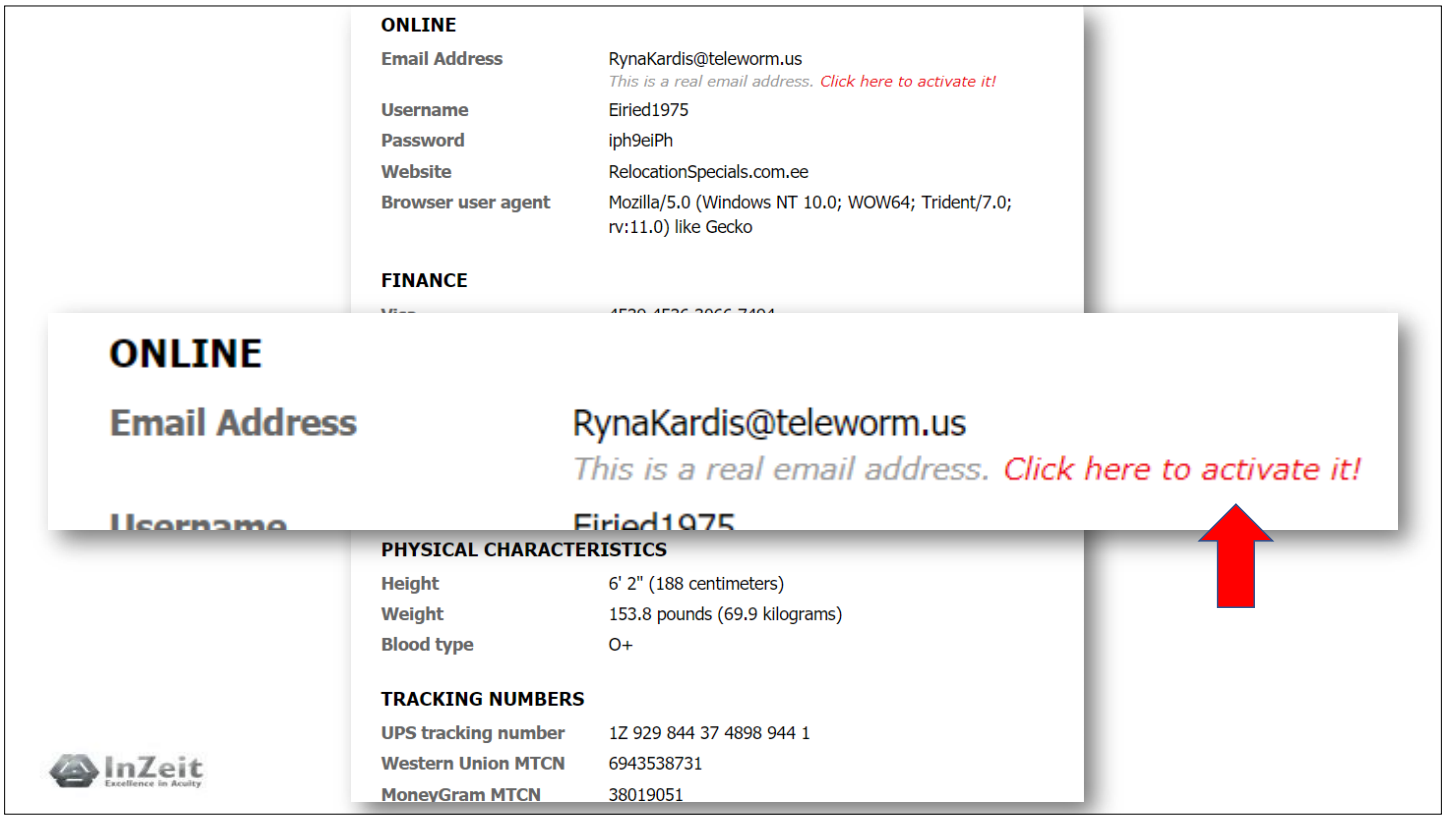
Use your imagination or …

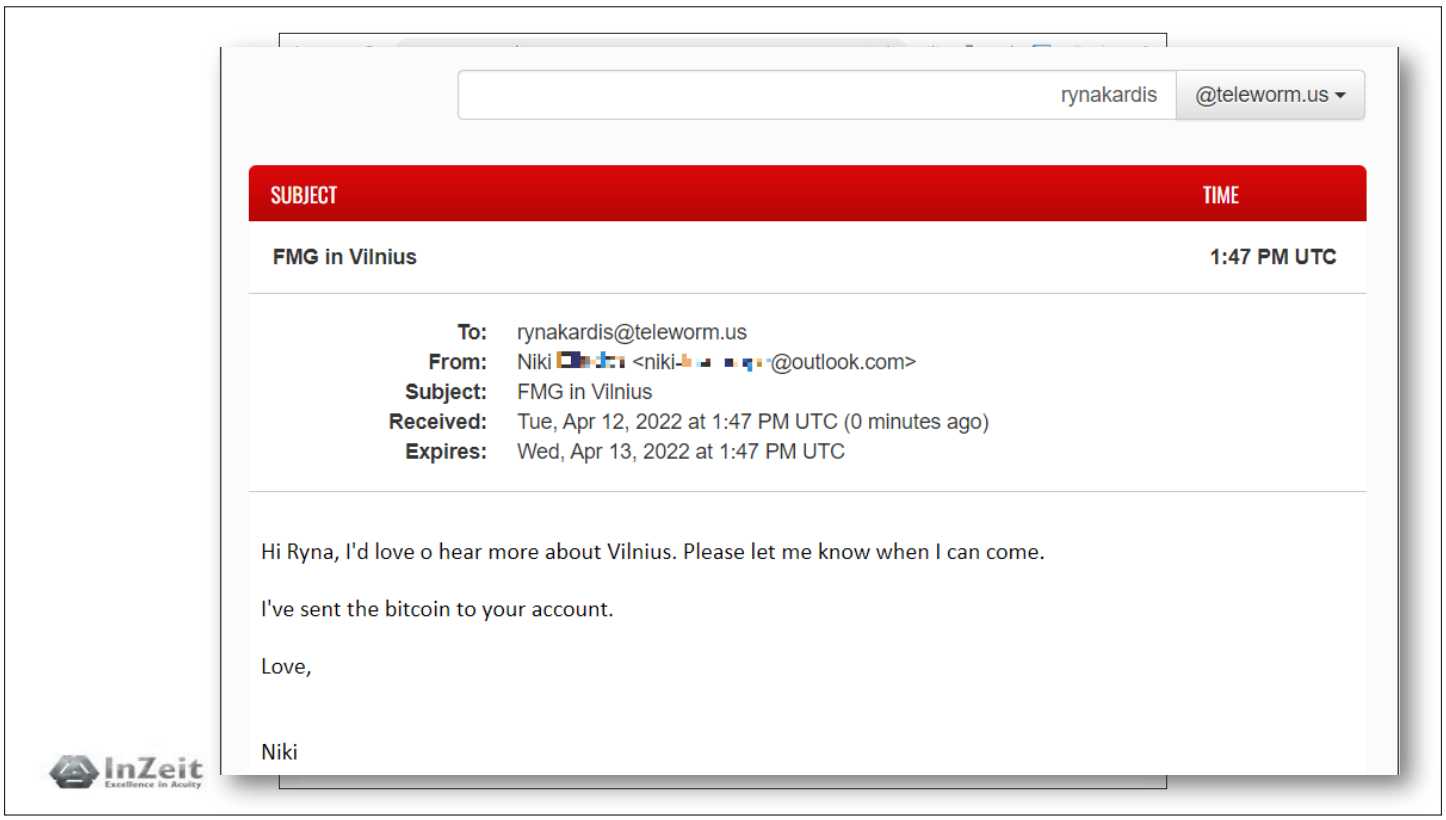
InZeit
Excellence in Acuity



fakenamegenerator.com

InZeit
Excellence in Acuity


ONLINE
Email Address
RynaKardis@teleworm.us
This is a real email address. Click here to activate it!
Username
Eiried1975
Password
iph9eiPh
Website
RelocationSpecials.com.ee
Browser user agent
Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
FINANCE
ONLINE
Email Address
RynaKardis@teleworm.us
This is a real email address. Click here to activate it!
Username
Eiried1975
PHYSICAL CHARACTERISTICS
Height
6' 2" (188 centimeters)
Weight
153.8 pounds (69.9 kilograms)
Blood type
O+
TRACKING NUMBERS
UPS tracking number
1Z 929 844 37 4898 944 1
Western Union MTCN
6943538731
MoneyGram MTCN
38019051
InZeit
Excellence in Acuity


rynakardis
@teleworm.us
SUBJECT
TIME
FMG in Vilnius
1:47 PM UTC
To: rynakardis@teleworm.us
From: Niki <niki-@outlook.com>
Subject: FMG in Vilnius
Received: Tue, Apr 12, 2022 at 1:47 PM UTC (0 minutes ago)
Expires: Wed, Apr 13, 2022 at 1:47 PM UTC
Hi Ryna, I'd love o hear more about Vilnius. Please let me know when I can come.
I've sent the bitcoin to your account.
Love,
Niki
InZeit
Excellence in Acuity

Using your Sock
= pseudonymity

With a sock social media account – interact with & research targets, view target's & family's social media history

Crooks can use it to look for weaknesses and craft a cyber attack

InZeit
Excellence in Acuity

Dog and Bone
(Cockney for phone)

Spy in your pocket

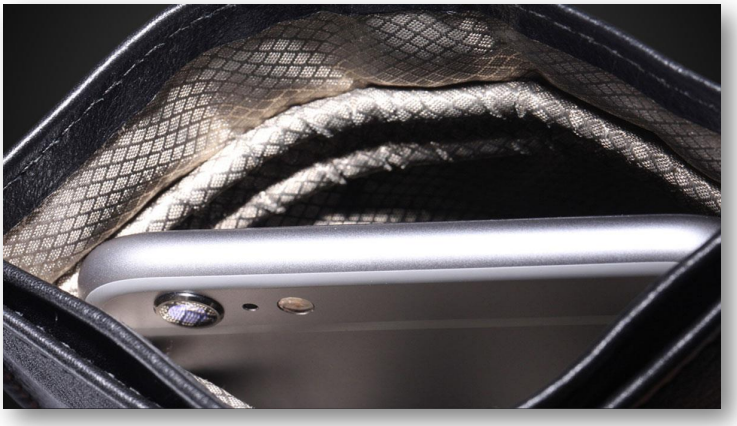
InZeit
Excellence in Acuity

Hiding the Dog

InZeit
Excellence in Acuity

If phone powered off or isolated (e.g. inside a Faraday bag or wrapped in metal foil), it can't be located.

Faraday bag = container lined with metallic substance to block radio waves



InZeit
Excellence in Acuity

Burner 'Pay-as-you-go' phones

Unregistered

Mask ID

Hiding the Dog

InZeit
Excellence in Acuity

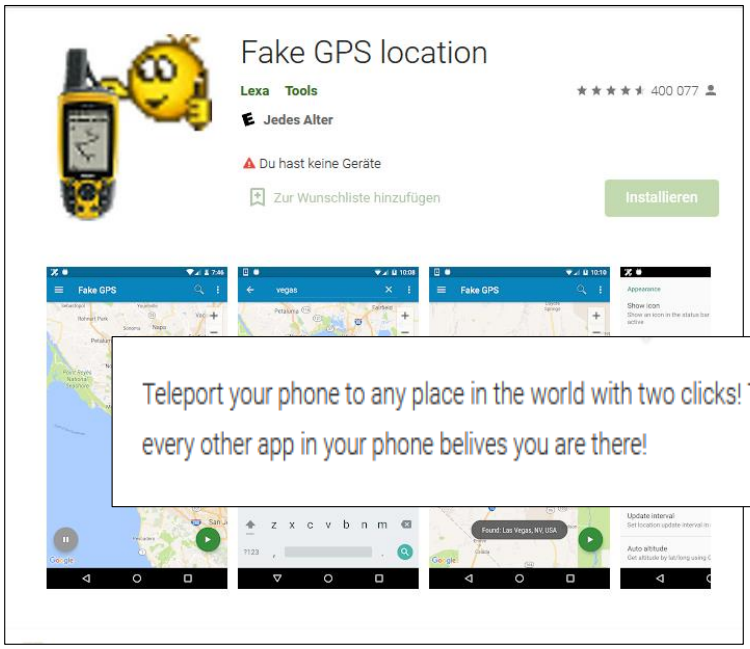
All phones have a unique International Mobile Equipment Identity (IMEI) number (alt. 'MEID')

Registered on network when connect

All SIM cards have an International Mobile Subscriber Identifier (IMSI) number

Identifies the subscriber to the telecoms provider

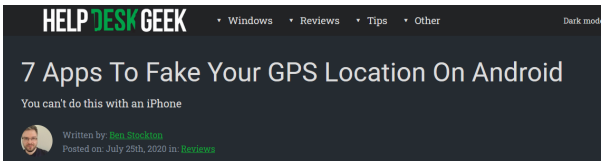
InZeit
Excellence in Acuity



UNTESTED

https://play.google.com/store/apps/details?id=com.lexa.fakegps&hl=de_AT&gl=US

https://helpdeskgeek.com/reviews/7-apps-to-fake-your-gps-location-on-android/



InZeit Excellence in Acuity

Bonfire of the Burners

195 countries in world 82% (about 160) require mandatory SIM-card registration with real name & personal data (Feb 2022)

30+ also require biometrics (e.g. fingerprints or facial scan)

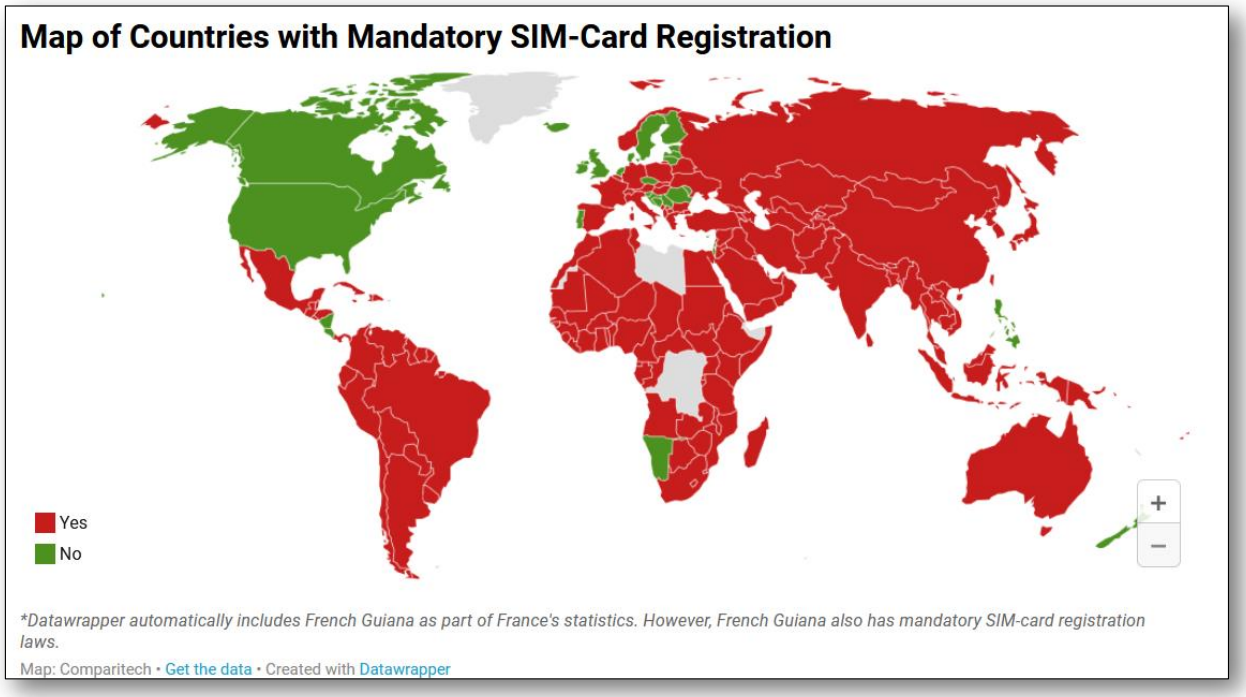
Bahrain, Bangladesh, Belarus, Benin, China, Ghana, Jordan, Lesotho, Mexico, Myanmar, Nigeria, Oman, Pakistan, Peru, Saudi Arabia, Singapore, Tajikistan, Tanzania, Thailand, Uganda, United Arab Emirates, Venezuela, and Zambia.

In preparation:
Ethiopia, Indonesia, Japan, Lebanon, Liberia, Jordan, Lebanon, Liberia, North Korea, & Russia.

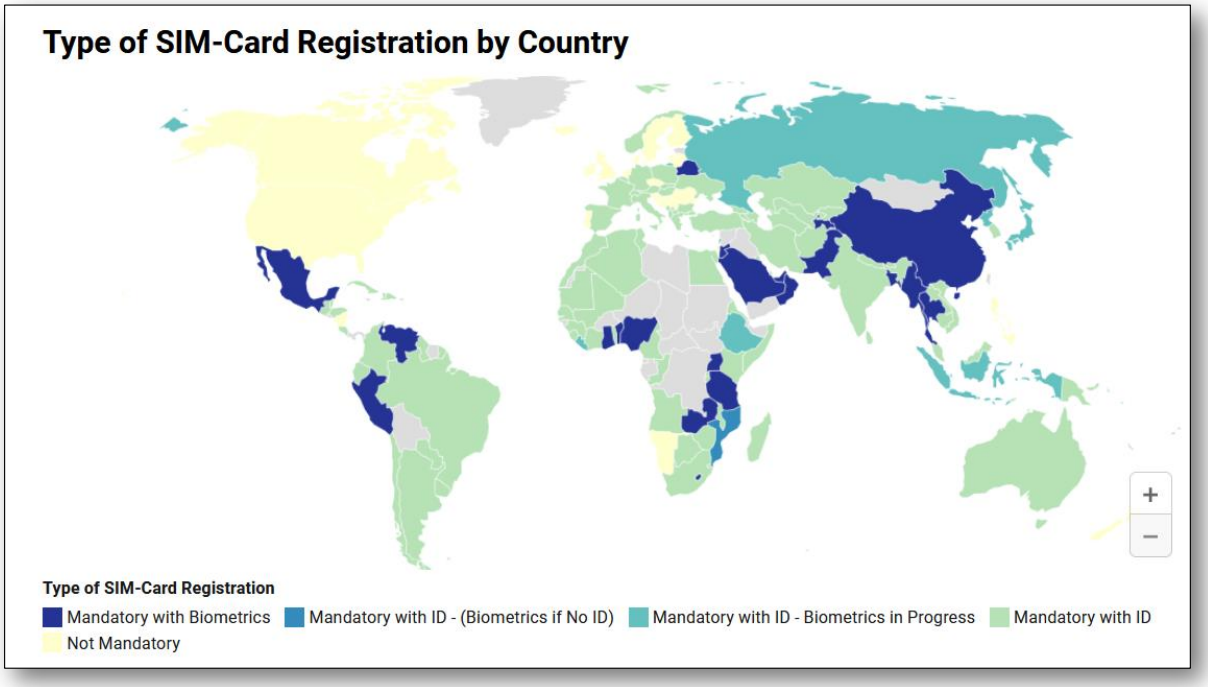
Mozambique, subscribers can provide their fingerprints if they don't have adequate ID.

InZeit Excellence in Acuity

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



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



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

Anonymous SIMs

In USA, Canada, Mexico can buy mintmobile SIM cards from Walmart, BestBuy & other Dept Stores for cash

But phone's unique IMEI number still registers with network

InZeit Excellence in Acuity

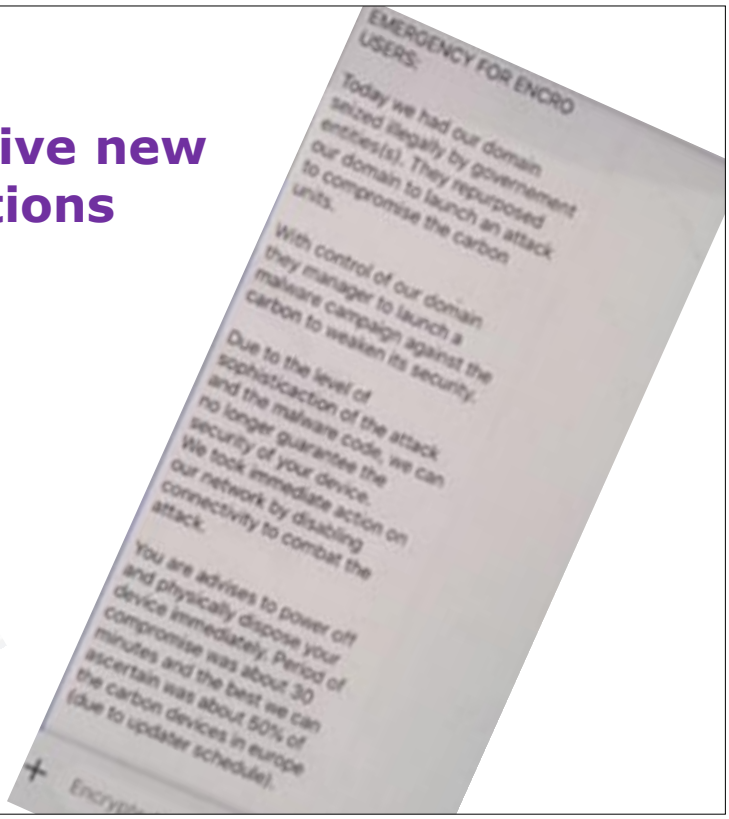
"MySudo is the all-in-one privacy app that lets you speak privately, browse privately and pay privately, all via secure digital profiles called Sudos. Each Sudo can have a secure phone number, handle, email, private browser and virtual card, so you can use your Sudo details instead of your own. Your personal information is safe since you haven't shared it — we won't even ask for a username or password to set up MySudo."

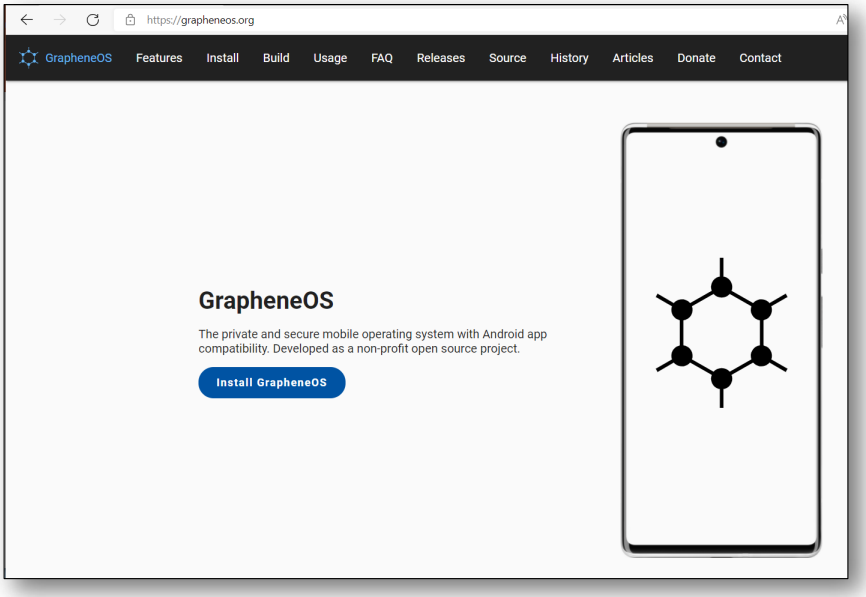
Australia Canada New Zealand Singapore South Korea United Kingdom USA

https://mysudo.com/

InZeit Excellence in Acuity

Alternative new solutions





The Privacy, Security, & OSINT Show – Episode 221

https://soundcloud.com/user-98066669/221-anonymous-mobile-devices

Hunting the Dog

Your phone sends signals to nearest cell-tower even on standby

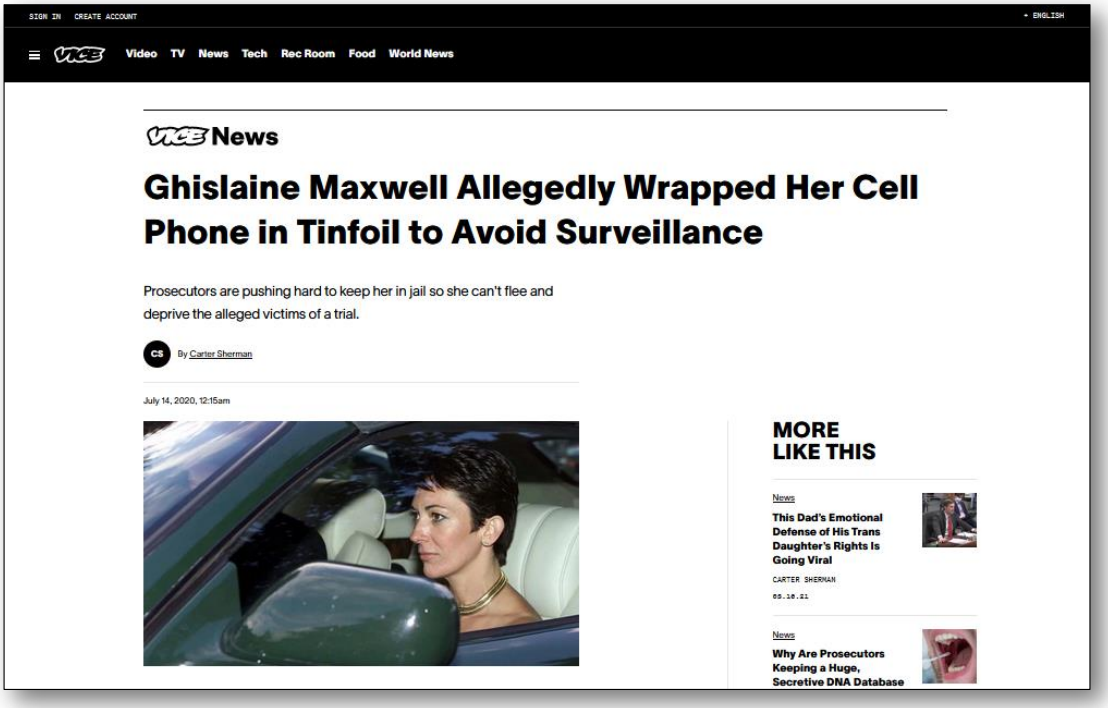
Allows cell-site analysis

Smartphones (may) have GPS

(It's all logged!!!)

InZeit
Excellence in Acuity

https://www.vice.com/en/article/pkyz3n/ghislaine-maxwell-allegedly-wrapped-her-cell-phone-in-tinfoil-to-avoid-surveillance



InZeit
Excellence in Acuity

IMSI Catcher

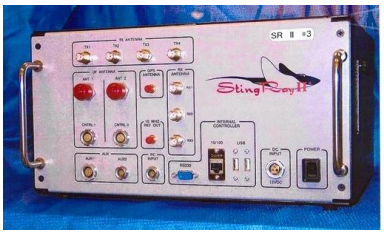
(aka StingRay, Hailstorm, TriggerFish)

Device imitates mobile phone base station

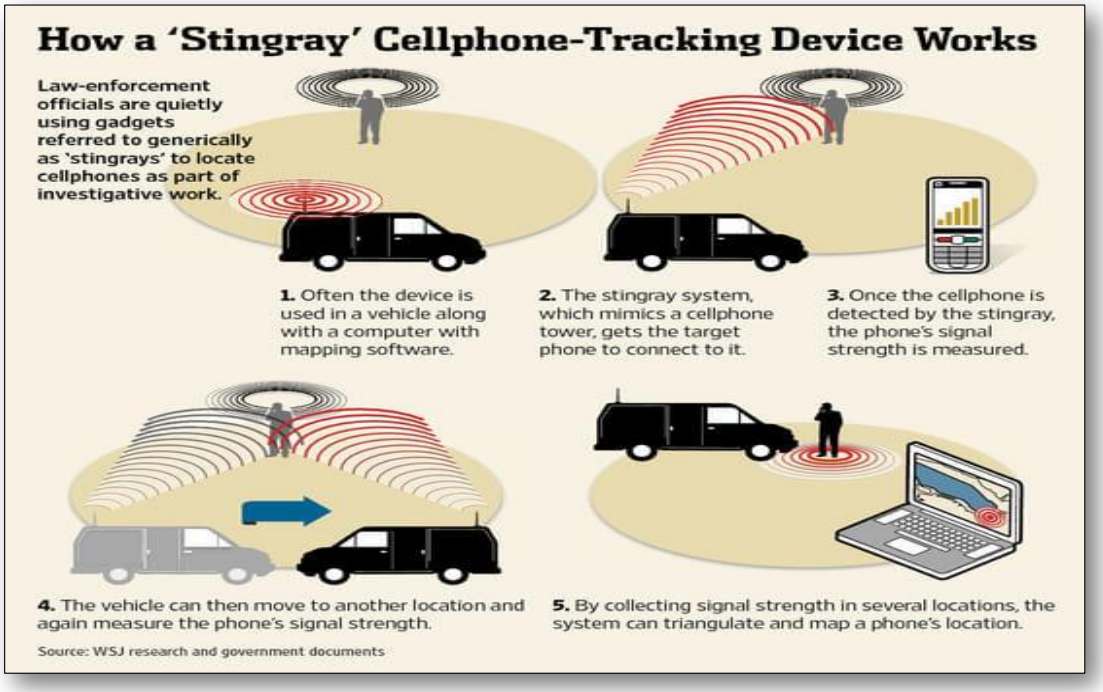
Phone automatically detects & connects to the IMSI catcher

All phone traffic passes through the IMSI catcher

Based on 2G technology, but 3G/4G phones are compatible (3G/4G signal can be disrupted or suppressed)

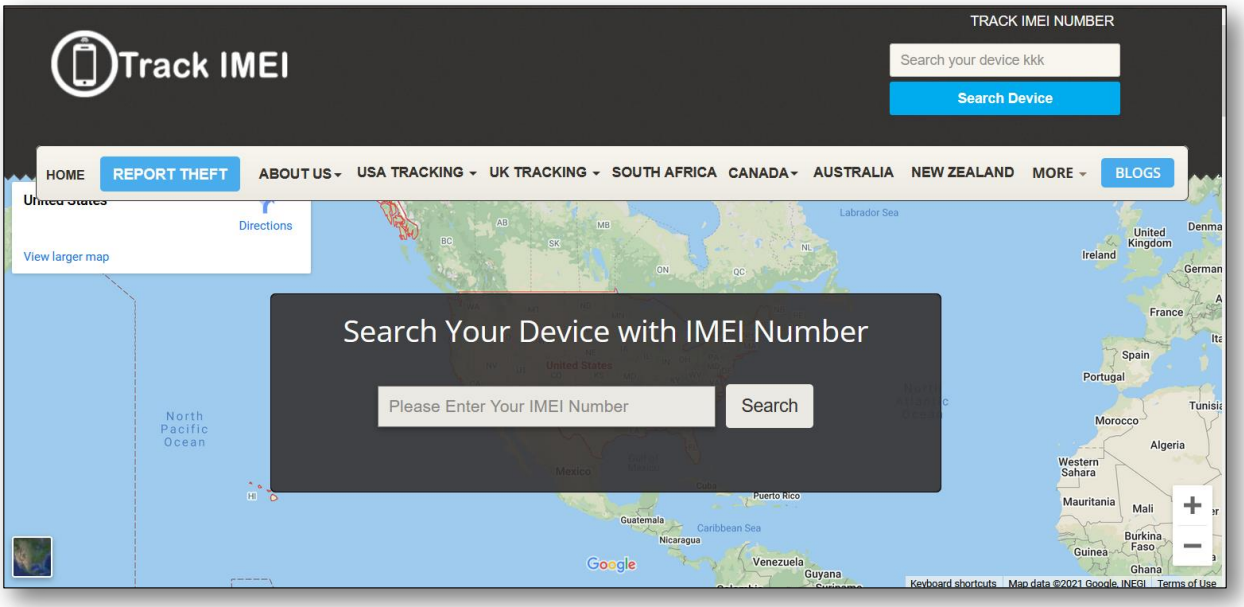


InZeit
Excellence in Acuity



InZeit
Excellence in Acuity

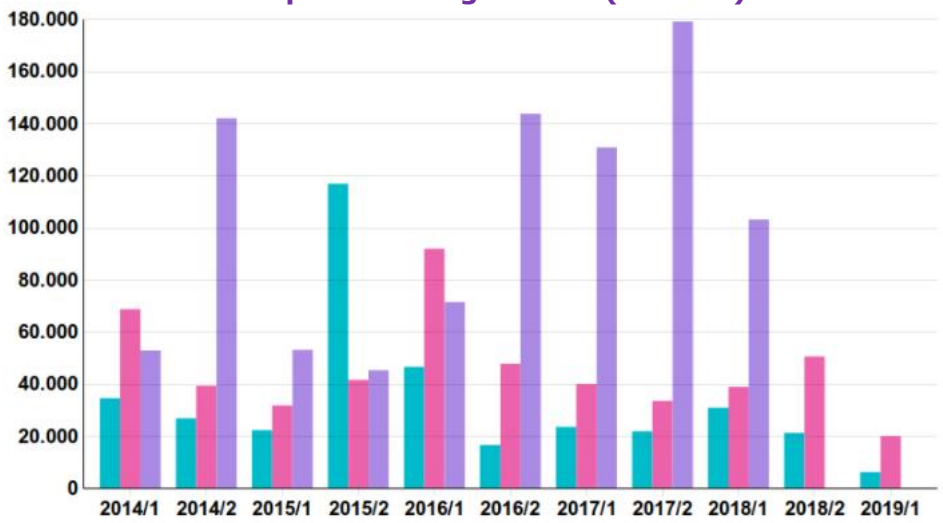
Source: https://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move



https://trackimei.net/

Stealth (SMS) Ping

Causes phone to register on (nearest) mast



BKA Federal Criminal Police
BPOL Federal Police
BfV Federal Office for the Protection of the Constitution

https://digit.site36.net/2019/08/20/less-stealth-sms-from-german-police-but-more-secrecy-for-domestic-intelligence/

- **'Попр-Д30.apk' Android Package developed by Ukrainian officer enabled rapid processing of targeting data for the Soviet-era D-30 Howitzer.**
- **Over 9,000 Ukrainian artillery personnel believed to use the app.**
- **Late summer 2016, CrowdStrike Intelligence analysts noticed 'Попр-Д30.apk' contained 'a number of Russian language artifacts that were military in nature'.**
- **2014 - 2016 'Попр-Д30.apk' had been infected ('trojanized') by FANCY BEAR .**
- **FANCY BEAR could intercept communications and identify locations from infected phones carried by Ukrainian artillery forces.**

InZeit Excellence in Acuity

https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

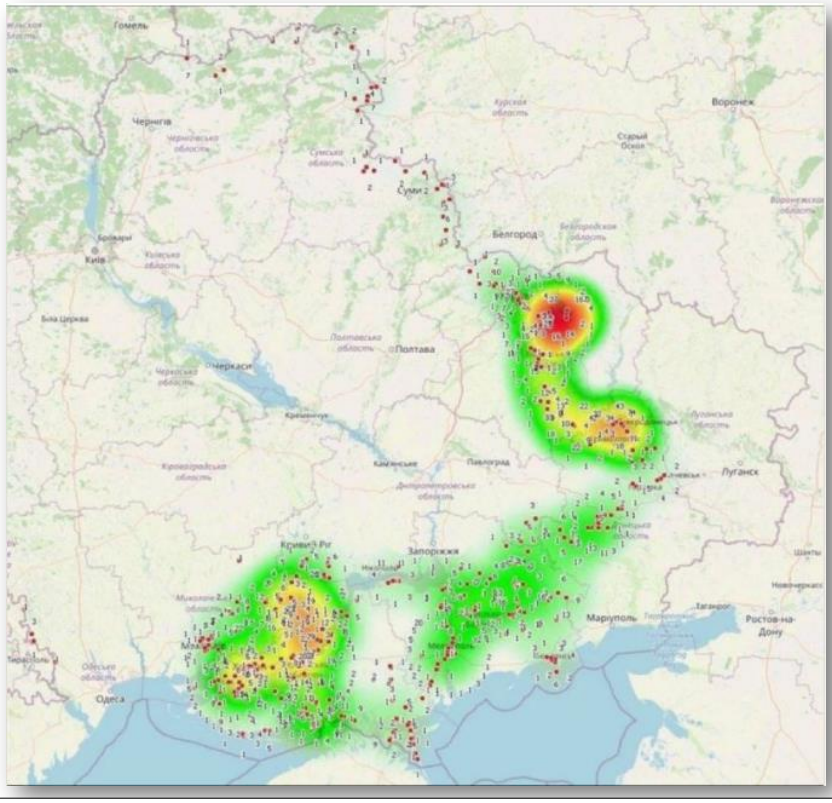
EXCLUSIVE: Russian spies are tracking British former special forces teams by their mobile numbers - and the data is then used to decide where to launch missile attacks

- **EXCLUSIVE: Kremlin has compiled a database of mobile phone numbers**
- **The information was gathered by spies near some of the UK's most sensitive military sites**
- **These include the headquarters of the Special Boat Service (SBS)**
- **Moment a mobile phone joins a local network their numbers are revealed to Russian agents**

By MARK NICOL DEFENCE EDITOR FOR THE DAILY MAIL
PUBLISHED: 22:01 GMT, 18 March 2022 | **UPDATED:** 22:34 GMT, 20 March 2022

https://www.dailymail.co.uk/news/article-10629125/Russian-spies-tracking-British-former-special-forces-teams-mobile-numbers.html

InZeit Excellence in Acuity



Active Russian SIM cards (May 2022)

Source: Dan Kaine, Inherent Risks

Geofence Warrants & Google's Sensorvault

52 billion people (almost 70% global population) have mobile phones

Who has an Android phone?

72.84% Android Global Market Share
(June 2021) statista.com

Location data saved to 'Sensorvault' database

InZeit
Excellence in Acuity

Sensorvault

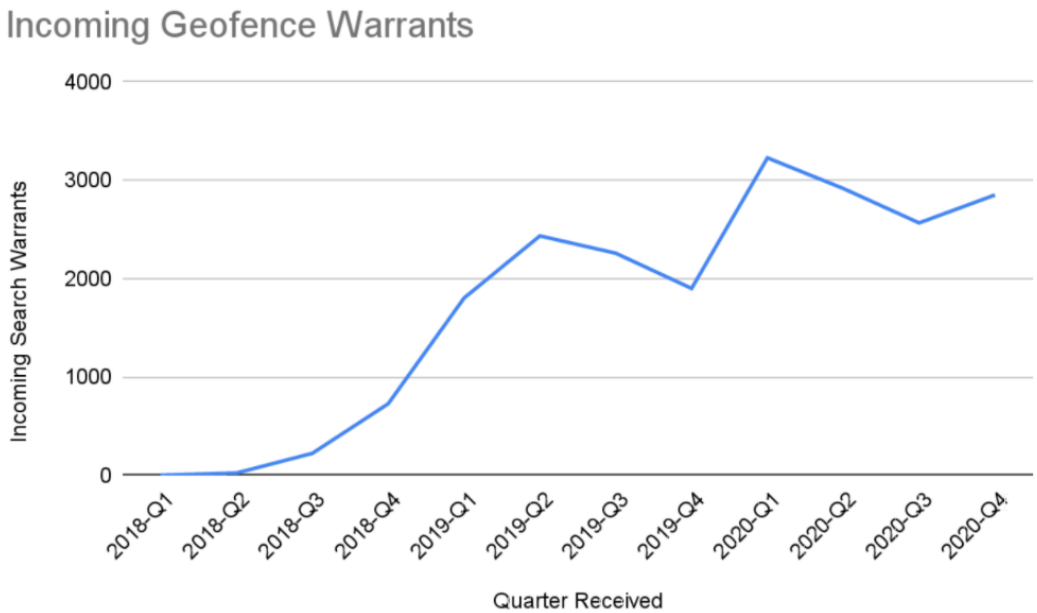
Google's Sensorvault database contains location data for hundreds of millions of devices all over the world.

'Geofence warrants' to Sensorvault can identify phones in vicinity of a crime.

Google Location History not enabled by default but users are prompted to enable it.

Initial data is anonymized, but once collated and analysed and potential suspect phones identified, Google provides the names of the owners of those devices.

InZeit Excellence in Acuity



25% of all US warrants received by Google in 2020

InZeit Excellence in Acuity

https://www.documentcloud.org/documents/21046081-google-geofence-warrants

Milwaukee, Wisconsin, USA June 2017

Middle of the night - Woman car jacked by 2 males

One drove, the other raped her. They stole her purse.

Victim saw the driver using google maps on his Smart Phone near General Mitchell International Airport

(Shortly before this attack another woman reported being followed nearby in dark pickup by two men who ran her off road and approached with a baseball bat)

InZeit
Excellence in Acuity

Geofence Warrant sought & obtained within 12 hours

Forwarded to Google flagged "exigent circumstances"

20 minutes later Google called back

Google assisted in refining the search, linking it to different locations involved

InZeit
Excellence in Acuity

Next night suspect used victim's credit card in a bar

Only one phone matched the three locations. Subscriber had previous conviction for 'unlawful imprisonment'

Police asked telecoms provider (T-Mobile) to track phone in real time.

Located in Louisville, Kentucky. Police arrested suspect after chase. Identified second suspect.

5 Days from crime report to arrest –DIFFERENT STATES.

InZeit Excellence in Acuity

https://www.nbcnews.com/news/us-news/she-didn-t-know-her-kidnapper-he-was-using-google-n1252472

Milwaukee to Louisville 400 miles (650km)

InZeit Excellence in Acuity

Issues:

Privacy

Users 'give permission' for their phones to be tracked

The tracking data is/are anonymised

Google acts as gatekeeper

'Blunt instrument'

Catches innocent bystanders, but Google vets data before divulging to police

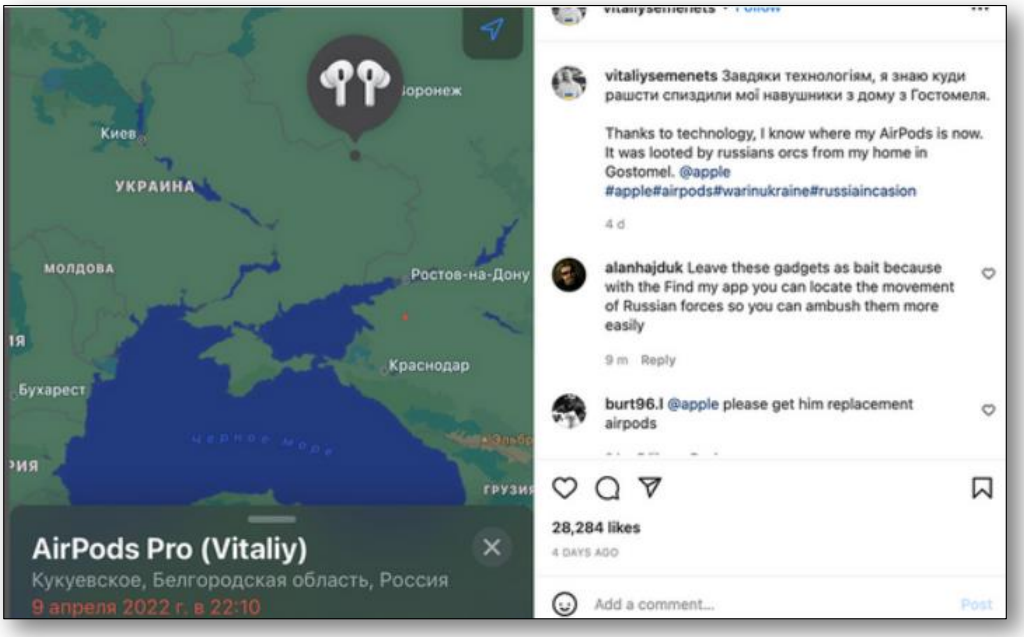
InZeit Excellence in Acuity

- **Gainsville Florida January 2020**
- **Keen cyclist**
- **RunKeeper Android App**
- **Email from Google**
- **'Will release data to Police unless get a court order preventing it'**
- **Burglary 97 year old woman's home (8 months before email sent)**
- **Passed 3 times in hour**

InZeit Excellence in Acuity

https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761

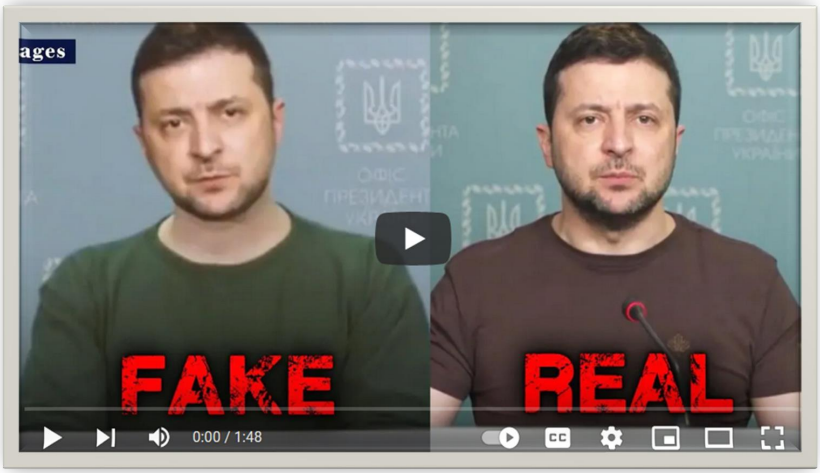
Not a phone, but Air Pods



https://www.express.co.uk/news/world/1597967/Russia-news-airpods-ukraine-war-find-my-apple-Hostomel-kyiv-retreat

Who do they think they are?

https://videos.dailymail.co.uk/video/mol/2022/03/18/7784774687089801062/1024x576_MP4_7784774687089801062.mp4



https://www.youtube.com/watch?v=enr78tJkTLE
(starts at 00:30 timestamp)

Deepfakes: *(a portmanteau of "deep learning" and "fake") are synthetic media in which a person in an existing image or video is replaced with someone else's likeness. (Wikipedia)*

Psychological harm	Financial harm	Societal harm
• (S)extortion • Defamation • Intimidation • Bullying • Undermining trust	• Extortion • Identity theft • Fraud (e.g. insurance/payment) • Stock-price manipulation • Brand damage • Reputational damage	• News media manipulation • Damage to economic stability • Damage to the justice system • Damage to the scientific system • Erosion of trust • Damage to democracy • Manipulation of elections • Damage to international relations • Damage to national security

Van Huijstee, M. et al (2021) "Tackling deepfakes in European policy"
https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2021)690039 p.6

InZeit Excellence in Acuity

video, audio or both

(in infancy, but already causing waves)

March 2019, (English Speaking) UK Director of a German Energy Company

Agitated CEO ordered immediate transfer of US$243,000 to current account in Hungary to cover last minute fee

https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

InZeit Excellence in Acuity

Transfer made, another phone call from CEO claiming it had been reimbursed.

A third call received requested a follow up payment

Suspicions aroused. Noticed call from an Austrian number.

As soon as Hungarian Bank received payment, funds transferred to Mexico and on to other countries …

https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

InZeit Excellence in Acuity

DeepFakes
Criminal Justice Risks:

Facilitate crime (esp. fraud)

…ence guilt

Issue: Understanding & Processing the technology!

…me the innocent

Create defence 'it wasn't me, it was a deep fake'

InZeit Excellence in Acuity

Cheer leader mom case

US competitive cheer-leading team (taken very seriously – code of conduct)

Doylestown, Pennsylvania: "Victory Vipers All Stars"

Team Coach received anonymous SMS with video of 16 y.o. Madi Hime vaping at a party

Clear violation of code of conduct

InZeit Excellence in Acuity

Images Source:https://www.dailymail.co.uk/news/article-9359823/Cheerleader-mom-created-deepfake-images-daughters-rivals-naked-drinking-smoking.html

Madi claimed it was fake – Mother reported to police

Also alleged Madi had received anonymous bullying texts and fake photos showing her naked and drinking alcohol

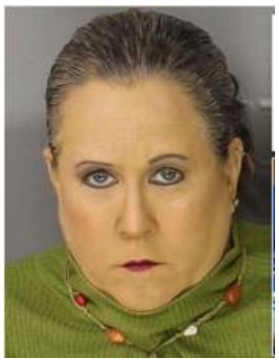
Mothers of two other squad members also made complaints of receiving anonymous texts about their children

One squad member received pictures of her daughter in a bikini with offensive captions superimposed

Another received texts alleging her daughter was smoking pot and drinking alcohol

InZeit Excellence in Acuity

Police traced texts to the Pinger platform and to the account of another mother: Raffaela Spone



Spone arrested on 6 counts of misdemeanour harassment and cyber-harassment of a child

InZeit
Excellence in Acuity

InZeit
Excellence in Acuity

Forensics expert found no trace of the texts, images or videos on Rafaella Spone's phone

Police admitted they never checked Madi (the victim's) phone

One of the alleged cyber-bullying texts was traced to 17 y.o. boy called Ethan

Henry Ajder, researcher and advisor on Deep Fakes, said

'very, very unlikely' someone without technical expertise could have produced such a deep fake … the vaping video would be 'borderline impossible'

InZeit Excellence in Acuity

25 March 2022, Rafaella Spone convicted of on three counts of misdemeano(u)r cyber harassment

.. No mention of DeepFakes

DeepFake? Or Real video?

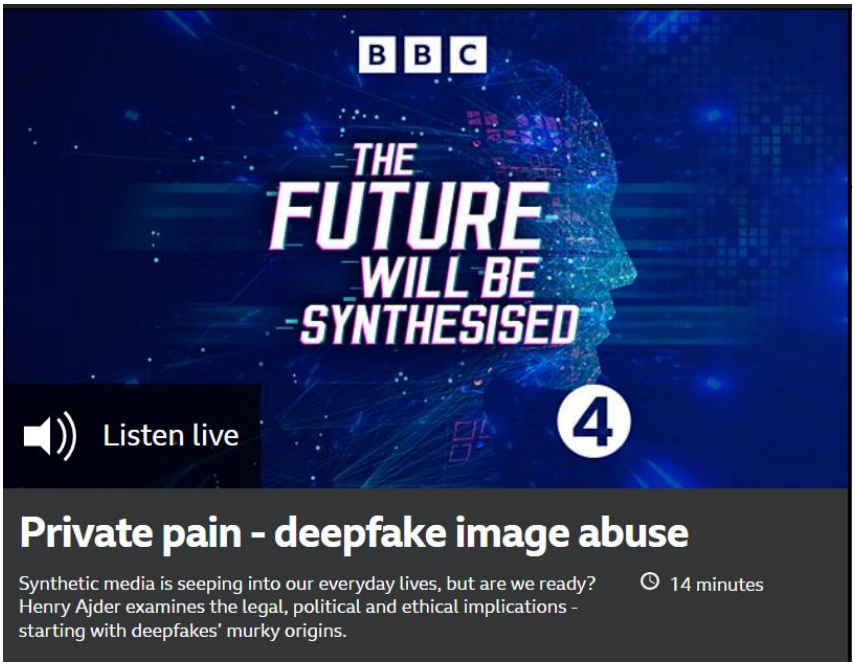
Inadequate procedures and evidence review

Carried away on technological paranoia?

No or no proper forensics

Could it happen in your country?

InZeit Excellence in Acuity



https://www.bbc.co.uk/programmes/m0017cpc

InZeit Excellence in Acuity

Keeping data private

User Authentication

Online payments

Encryption

If intercepted, data can't be read

Protocols for Internet

Works for honest & dishonest

VPNs

Confidential communications

InZeit Excellence in Acuity

What does 'hash' mean?

A. chopped food specifically: chopped meat mixed with potatoes and browned

B. a restatement of something that is already known; the same old hash

C. hodgepodge, jumble

D. Pound sign (#)

E. Cannabis

InZeit Excellence in Acuity

https://www.merriam-webster.com/dictionary/hash

Hashing

(Technically not encryption)

Application of a complex mathematical equation ('Hashing algorithm') to data

Result = hash value ('irreversible maths')

Unique alphanumeric string of characters of fixed length (data 'fingerprint')

Different algorithms produce different length hash

InZeit Excellence in Acuity

Hash Value: long string of letters & numbers

Used in:

Identifying malware

Digital forensics for checking duplicated data

Storing passwords

InZeit
Excellence in Acuity

Popular Hashing Algorithms:

- **Message Digest MD5**
- **Secure Hashing Algorithm (SHA1, SHA256, SHA 512)**
- **BCrypt**

InZeit
Excellence in Acuity

This online tool allows you to generate the SHA256 hash of any string. SHA256 is designed by NSA, it's more reliable than SHA1.

Enter your text below:

mysecretpw

Generate | Clear All | MD5 | SHA1 | SHA512 | Password Generator

☐ Treat each line as a separate string ☐ Lowercase hash(es)

SHA256 Hash of your string: [Copy to clipboard]

EA567ED0B110B8E9E4642CA3EBC00B1C3EA8688E97A3B33634E05902FB8A4364

InZeit Excellence in Acuity

https://passwordsgenerator.net/sha256-hash-generator/

This online tool allows you to generate the SHA256 hash of any string. SHA256 is designed by NSA, it's more reliable than SHA1.

Enter your text below:

Mysecretpw

Generate | Clear All | MD5 | SHA1 | SHA512 | Password Generator

☐ Treat each line as a separate string ☐ Lowercase hash(es)

SHA256 Hash of your string: [Copy to clipboard]

019A74A3E170B374E0EA25C9C56382A550C069790D70E92F014D23358F4C93B9

EA567ED0B110B8E9E4642CA3EBC00B1C3EA8688E97A3B33634E05902FB8A4364

InZeit Excellence in Acuity

https://passwordsgenerator.net/sha256-hash-generator/

Antivirus software compares the hash values ('data fingerprints') of data downloaded or stored on your device with a list of hash values of known malware

InZeit
Excellence in Acuity

Hashing Passwords

Good practice:
Passwords should not be stored in cleartext
Should be 'Hashed' – hashes can't be 'cracked'

Good practice:
Block login after x number of failed attempts
Multi-factor authentication

InZeit
Excellence in Acuity

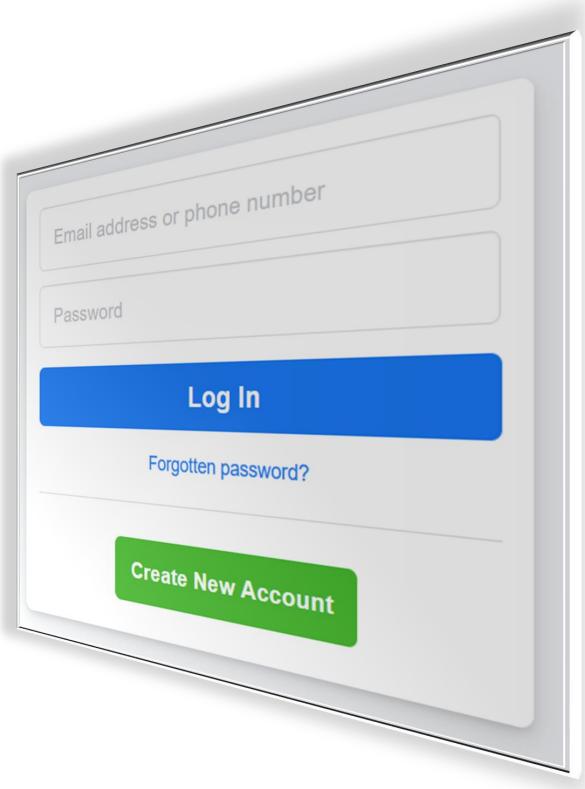
Login

Enter Username/Email

Enter Password

Your input hashed

If matches the hash on record against username , given access



InZeit
Excellence in Acuity

Cracking passwords:

Practical:

- Brute-forcing
- Rainbow (Lookup) Tables
- Malware (e.g. Pegasus)
- Comb Data breaches
- Checking crime scene

InZeit
Excellence in Acuity

Hashes can't be cracked, but can be compared

Find it written down at crime scene

Ask the owner *(nicely!)*
Brute force
(use every possible combination of chars 1 by 1)

Make a list of possible passwords
(from a dictionary/target research)

Hash them

Rotate each hash against the login
If the password/hash is on the list, access granted

Previous breached data (on Darknet)

Cracking passwords:

Policy & Legal

- **Key Disclosure Law**
- **Key Escrow**
- **Official Backdoors**
- **Client-Side Scanning**

s49 RIPA
https://www.legislation.gov.uk/ukpga/2000/23/part/III/crossheading/power-to-require-disclosure

Client Side Scanning

https://www.europol.europa.eu/media-press/newsroom/news/146-children-worldwide-saved-in-operation-targeting-child-abuse-online?mtm_campaign=newsletter

The problem: End to end encryption

Data encrypted in transit

Proposed solution: scan data on sender's device before encryption

Apple introduced in USA in August 2021 to scan photo libraries on iPhones. Ceased 3rd Sept 2021.

Obligatory & Indiscriminate

Scope for abuse?

InZeit Excellence in Acuity

"The EU wants to oblige providers to search all private chats, messages, and emails automatically for suspicious content – generally and indiscriminately. The stated aim: To prosecute child pornography. The result: Mass surveillance by means of fully automated real-time messaging and chat control and the end of secrecy of digital correspondence."

Patrick Breyer MEP

11 May 2022: Presentation of Commission proposal on mandatory messaging and chat controls for online service providers (tbc)

InZeit Excellence in Acuity

https://www.patrick-breyer.de/en/posts/messaging-and-chat-control/

Court of Justice of the European Union
PRESS RELEASE No 58/22
Luxembourg, 5 April 2022

Press and Information

Judgment in Case C-140/20
Commissioner of An Garda Síochána and others

The Court confirms that EU law precludes the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime

The national court may not impose a temporal limitation on the effects of a declaration of invalidity of a national law that provides for such retention

(Compare Google's Sensorvault)

https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-04/cp220058en.pdf

References & Resources

InZeit Excellence in Acuity

Client side scanning

Breyer,P.(2022) *Chat Control* https://www.patrick-breyer.de/en/posts/messaging-and-chat-control/

Ducket, C. (2021) Apple is bringing client-side scanning mainstream and the genie is out of the bottle https://www.zdnet.com/article/apple-is-bringing-client-side-scanning-mainstream-and-the-genie-is-out-of-the-bottle/

EDRI (2022) EU Rules on Scannin gPrivate Online Communications: document pool https://edri.org/our-work/eu-rules-on-scanning-private-online-communications-document-pool/

EU Parliament letter to Commission (2022) https://www.patrick-breyer.de/wp-content/uploads/2022/01/20220127_COM-letter-chatcontrol.pdf

European Court of Justice (2022) Press Release Judgment in Case C-140/20 https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-04/cp220058en.pdf

Europol (2022) *146 children worldwide saved in an operation targeting child abuse online* https://www.europol.europa.eu/media-press/newsroom/news/146-children-worldwide-saved-in-operation-targeting-child-abuse-online?mtm_campaign=newsletter

InZeit Excellence in Acuity

Internet Society (2020) *Fact sheet:Client-Side Scanning*
https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/

Rozenzweig,P. (2020) ***T**he Law and Policy of Client-Side Scanning*
https://www.lawfareblog.com/law-and-policy-client-side-scanning

Vagle,J. (2021) *Client-Side Scanning: A New Front In the War on User Control of Technology*
https://www.justsecurity.org/78749/client-side-scanning-a-new-front-in-the-war-on-user-control-of-technology/

Deep Fakes

Korducki K.M (2021) *The World Thought This Cheer Mom Created a Deepfake to Harass Her Daughter's Rival—but the Real Story Is Way More Confusing (and Bizarre)*
https://www.cosmopolitan.com/lifestyle/a37377027/deep-fake-cheer-scandal/

Harwell, D. (2021*) Remember the 'deepfake cheerleader mom'? Prosecutors now admit they can't prove fake-video claims*
https://www.washingtonpost.com/technology/2021/05/14/deepfake-cheer-mom-claims-dropped/

Stupp, C (2019) *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*
https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Zelinsky fake video https://www.youtube.com/watch?v=enr78tJkTLE

Van Huijstee, M. et al (2021) *Tackling deepfakes in European policy*
https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2021)690039 p.6

InZeit Excellence in Acuity

Sock Puppets

https://receive-smss.com

https://thispersondoesnotexist.com

https://fakenamegenerator.com

Encryption

Regulation of Investigatory Powers Act 2020 Art 49
https://www.legislation.gov.uk/ukpga/2000/23/part/III/crossheading/power-to-require-disclosure

Passwords
https://crackstation.net
https://hashes.com/en/tools/hash_identifier
https://passwordsgenerator.net/sha256-hash-generator/

InZeit

Phone tracking

Donnelly,D.(2022) *Russia's Kyiv retreat captured by stolen AirPods as bumbling troops give positions away* https://www.express.co.uk/news/world/1597967/Russia-news-airpods-ukraine-war-find-my-apple-Hostomel-kyiv-retreat

Fake GPS Location
https://play.google.com/store/apps/details?id=com.lexa.fakegps&hl=de_AT&gl=US

Mayers.A.(2016) *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units*
https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units

Stockton,B. (202o) 7 apps to fake your GPS location on android
https://helpdeskgeek.com/reviews/7-apps-to-fake-your-gps-location-on-android/

SIM Card Registration

Privacy International (2019) https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws

Bishoff,P. (2022) *Which governments impose SIM-card registration laws to collect data on their citizens?* https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/

Bazzell,M. *The Privacy, Security, & OSINT Show – Episode 221*
https://soundcloud.com/user-98066669/221-anonymous-mobile-devices

InZeit

GEORGE M.R. ZLATI

- Lawyer in private practice (Romania)
  - 10 years experience in cybercrime
- PhD in Cybercrime
  - „Unauthorized access to a computer system, computer fraud and computer forgery”
- Teaching Criminal Law & Cybercrime

SCAN ME

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

1

Search and seizure of stored computer data. Technical and legal aspects

- ECHR Jurisprudence
- Computer systems & storage mediums
- Volatile & non-volatile data
- The problem of timestamps
- Interpreting digital evidence

2

1. Cybercrime 1.0 vs. Cybercrime 2.0
2. We are not prepared! (are we?)

Disclaimer: We are doomed

3

Case law of the European Court of Human Rights

1. Wieser and Bicos Beteiligungen GMBH v. Austria **(2008)**
2. Robathin v. Austria **(2012)**
3. Nagla v. Latvia **(2013)**
4. Sérvulo & Associados - Sociedade de Advogados, Rl v. Portugal **(2015)**

4

- The Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents (...) **these provisions also apply to the search and seizure of electronic data**.

  → SEALING OF THE BIT-STREAM IMAGE

- **Effective safeguards against any abuse and arbitrariness**: the search was based on a warrant issued by a judge; **the scope of the warrant was reasonably limited**; the search was carried out in the presence of an independent observer in order to ensure that materials subject to professional secrecy were not removed.

Wieser and Bicos *v.* Austria

- Violation of article 8

5

Arguments for not sealing the bit-stream image:

- There is a hash value (e.g. MD5, SHA-1 etc.) generated from the bit-stream image... so there is no risk!

Arguments against not sealing the bit-stream image:

- ...You can access the image covertly after the warrant has expired
- ...You can obtain information covertly even if the activity is not covered by the warrant

  → Exploratory search

Real world problem #1

6

- The **scope of the warrant and purpose of the warrant was very broad**, since it referred to documents, saving books, wills etc.
  - Avoiding blanket search warrants (risk of exploratory search)
- The police officers who conducted the search **copied all files** from the applicant's computer to discs.
  - The difference between creating a bit-stream image (acquisition process) and collecting the digital evidence as the last step of the procedure

Robathin *v.* Austria

- Violation of article 8

7

"Regarding the request for exclusion of evidence obtained by violating article 8 of the Convention, as a consequence of a blanket warrant (...) the interference with the right to privacy can be analyzed only *in concreto* (...) even if there was a blanket warrant, the computer search was executed only with the scope to obtain digital evidence relevant to the investigation.

Cluj Court of Appeal, 2017

Real world problem #2

8

- The **existence of reasonable suspicion is to be assessed at the time of issuing the search warrant**. (...) The fact that the applicant was eventually acquitted years later cannot change this assessment.

  Search warrant in a computer fraud case & you find digital evidence only for child pornography. If you stop the investigation for computer fraud you can still use the evidence for child pornography.
  (not in case of an exploratory search)

Robathin *v.* Austria

- Violation of article 8

9

- The search warrant was drafted in such **vague terms** as to allow the seizure of „any information".

  If you know what you are searching for you should know what to ask for

Nagla *v.* Latvia

- Violation of article 10
- Journalism

10

Effective safeguards against any abuse and arbitrariness:

- There was a **warrant** for the computer search and seizure of computer data;
- There was an **ex-ante and ex-post control** by the investigating judge;
- The scope of the search and seizure **warrant was broad** (35 generic keywords have been used) **BUT**
  - The investigating judge ordered the **deletion of 850 records** which he considered to be private, covered by the professional secrecy or to have no direct bearing on the case.

Effective legal remedy

Sérvulo & Associados *v.* Portugal

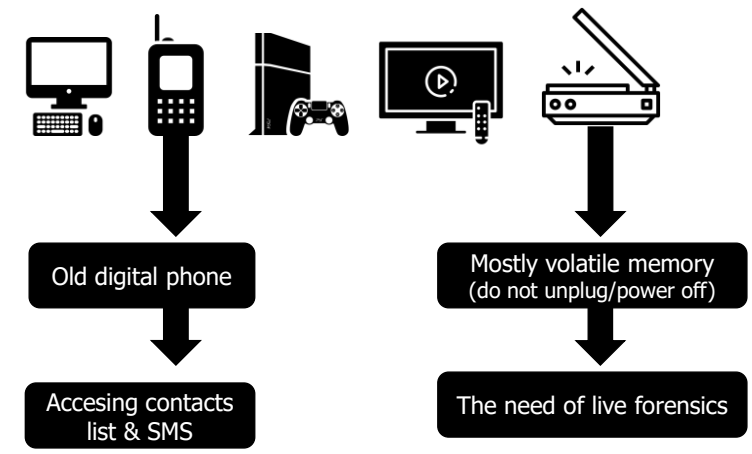
- No violation of article 8
- The case concerned the search of the law firm's office and the seizure of computer files and email messages

11

- The scope of the computer search **warrant cannot be vague or too broad**;
  - The prosecutor must specify what computer data (digital evidence) he is looking for and limit the interference with the right to private life;
- The individual who executes the computer search warrant **cannot copy all/most of the data** on a storage medium device under the control of the investigation body;
  - There is a difference between the creation of the bit-stream image/bit-by-bit image/clone (the acquisition process) and the collecting of digital evidence as the final step in the computer search and seizure procedure;
- **The bit-stream image should be sealed** at the end of the procedure;
  - Mitigating the risk of accessing the content of the image covertly and outside the limits of the warrant.

Concluding remarks

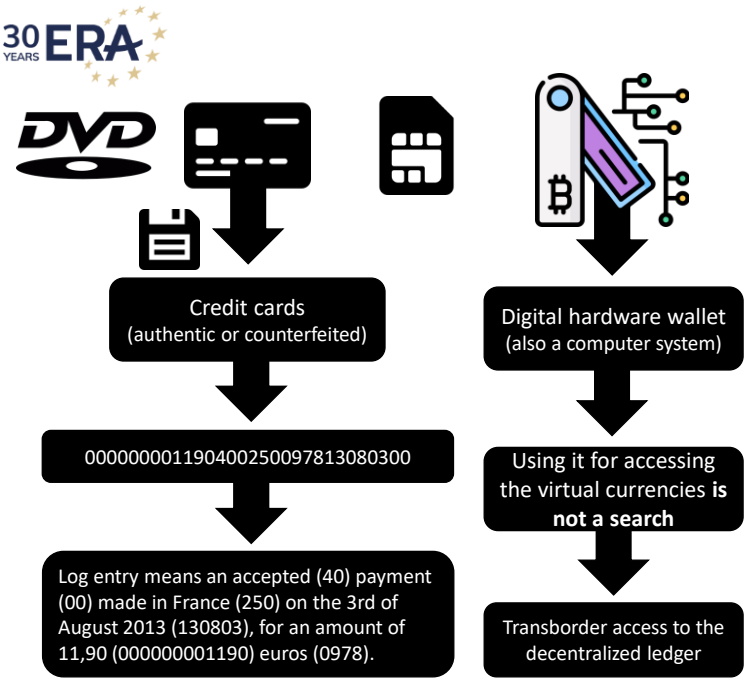
12



Computer systems

- From old to new
- Any device that can process computer data by using a computer program
- Evidentiary value
- **The need for a warrant**

13



Storage mediums

- From old to new
- If it can store computer data it is a storage medium
- Evidentiary value
- **The need for a warrant**

14

Contents lists available at ScienceDirect

Digital Investigation

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

Payment card forensic analysis: From concepts to desktop and mobile analysis tools

T. Souvignet [a, b, *], J. Hatin [c], F. Maqua [a], D. Tesniere [c], P. Léger [c], R. Hormière [d]

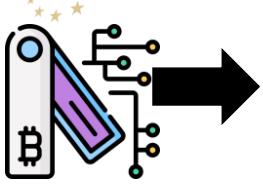
[a] Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), Digital Forensics Department (INL), 1 boulevard Théophile Sueur, 93110, Rosny-Sous-Bois, France
[b] PRES Sorbonne Universités – Université Panthéon-Assas Paris II, 12 place de Panthéon, 75005, Paris Cedex 05, France
[c] ENSICAEN, 6 boulevard maréchal Juin, 14050, Caen Cedex 4, France
[d] INSA Lyon, 20 avenue Albert Einstein, 69100, Villeurbanne, France

> Thus EMV provides an interesting feature for investigators: log entries. By "provid[ing] support for accessing a transaction log file by special devices" (EMV book 3, 2011), some EMV payment cards offer a variable size payment and withdrawal history.

Real world problem #3

- Two counterfeited cards
- Two different holders
- One withdrawal from the ATM
- Who done it?

15

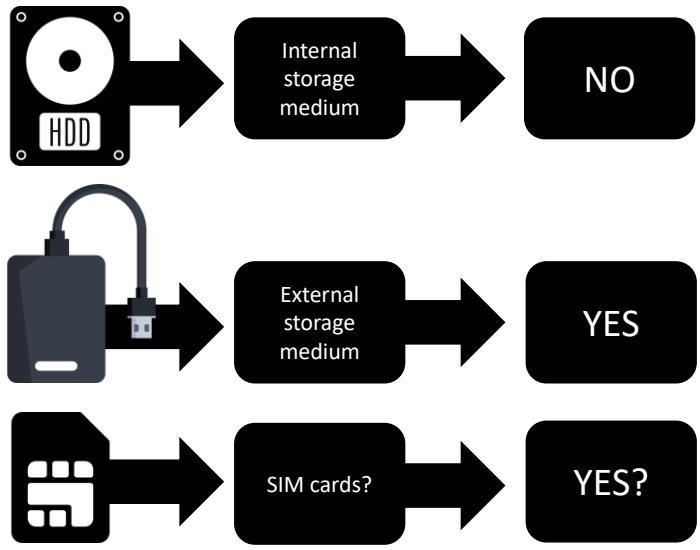


"Key" for accessing the virtual currencies stored in the blockchain

> **Trans-border access to stored computer data with consent or where publicly available**
> A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically;
> **Article 32 – Cybercrime Convention**

Real world problem #4

16



Do you need a warrant for both the computer system and the data storage medium?

17

The warrant: „searching the iPhone 4 device with IMEI no. ### containing a SIM card with the phone number ###".

- Was the SIM card covered by the warrant?
- Is the SIM card part of the smartphone?
- Is the SIM card just an additional criterion for identifying the iPhone?

Real world problem #5

18

(...) the judge of rights and liberties issued a warrant both for the search of the mobile phone and of the SIM card, thus we reject the argument according to which the reference made to the SIM card was only an additional criterion for identifying the mobile phone (...)

Cluj Court of Appeal, 2017

Real world problem #6

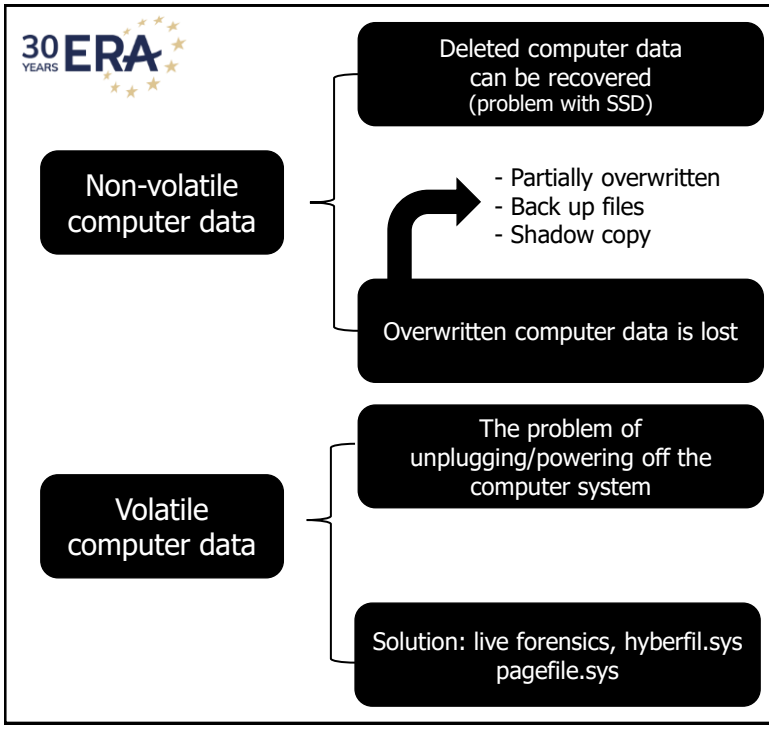
19

The warrant makes a generic reference to the computer systems only by identifying them as laptops or desktops. The warrant does not even refer to the rooms where the computer systems were located (...)

Cluj District Court, 2022

Real world problem #7

20



Volatile data *vs* Non-volatile data

- How to acquire data
- How to recover data

21

Timestamps

- What are they?
  - Metadata
- Are they reliable?
  - Not really

M: Last data **modification** stamp (only the content of the file)

A: Last **access** timestamp (can be done by the OS)

C: Last file **change** timestamp (e.g. author of the file)

File creation date is a different timestamp (can change by copying the file in a different source)

22

- Timestamps can be easily tampered;
  - *Touch* command in Linux;
- The creation timestamp can be after the last; access timestamp;
  - The file was accessed and then copied;
- The timestamps can be modified by the OS;
- Sometimes the timestamps do not change;
  - Difference between OS or softwares;

Timestamps

- What are they?
  - Metadata
- Are they reliable?
  - Not really

23

86.120.169.XX - r34372pmla [06/09/2021:14:41:00-0000] "POST /cpsess7965786446/execute/Email/passwd_pop HTTP/1.1" 200 0 "https://server-0340.whmpanels.com:2083/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.2 Safari/605.1.15" "s" "-" 2083

Digital evidence in CPANEL logs

- Checking CPANEL documentation
- Interpreting the logs correctly

24

86.120.169.XX [IP used by the attacker] - r34372pmla [**06/09/2021:14:41** DATE:00-0000] "POST /cpsess7965786446/**execute/Email/passwd_pop** [change of e-mail account password] HTTP/1.1" 200 0 "https://server-0340.whmpanels.com:2083/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.2 Safari/605.1.15" "s" "-" **2083** [port for CPANEL]

- ✓ The attacker used CPANEL
- ✓ From XXX IP address
- ✓ In order to change the password to an e-mail account
  - ➢ Alteration of computer data
  - ➢ Restricting access to computer data

Digital evidence in CPANEL logs

- Checking CPANEL documentation
- Interpreting the logs correctly

25

86.120.169.XX - r34372pmla [06/09/2021:14:51:58-0000] "GET /cpsess7965786446/frontend/paper_lantern/mail/**webmailform.html?user=contact%40zlati.legal** [what e-mail account was accessed without authorization] &return_request_uri=%2Fcpsess7965786446%2Ffrontend%2Fpaper_lantern%2Femail_accounts%2Findex.html HTTP/1.1" 200 0 "https://server-0340.whmpanels.com:2083/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.2 Safari/605.1.15" "s" "-" 2083

- ✓ The attacker used CPANEL
- ✓ From XXX IP address
- ✓ In order to access an e-mail account
  - ➢ Unauthorized access to a computer system

Digital evidence in CPANEL logs

- Checking CPANEL documentation
- Interpreting the logs correctly

26

86.120.169.95 - r34372pmla [06/15/2021:16:55:54-0000] "GET /cpsess9468514199/frontend/paper_lantern/mail/**dodelfwd.html?email=contact%40zlati.legal&emaildest=george.zlati%40protonmail.com** [deleting the forward email instruction] HTTP/1.1„ (...)

- ✓ The attacker used CPANEL
- ✓ From XXX IP address
- ✓ In order to delete the e-mail forward instruction
  - ➢ Alteration of computer data
  - ➢ Restricting access to computer data

Digital evidence in CPANEL logs

- Checking CPANEL documentation
- Interpreting the logs correctly

27

Location

AppData › Local › Microsoft › Windows › Explorer

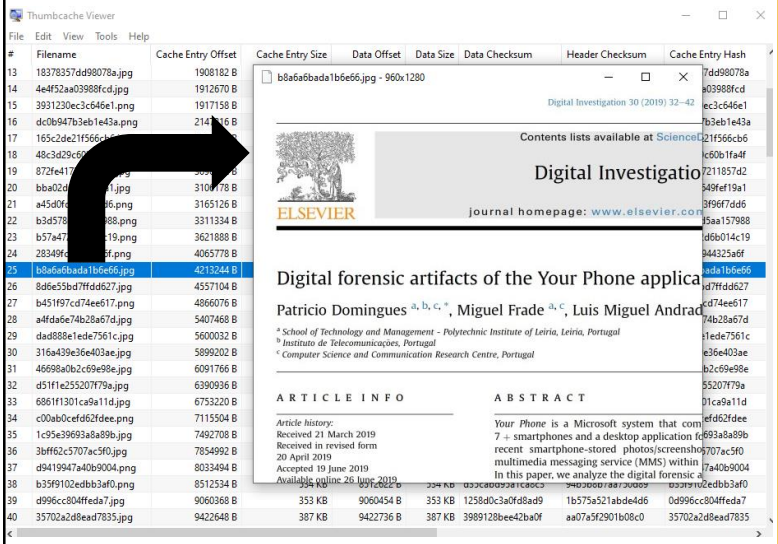
Thumbnail size

Name	Date modified	Type	Size
thumbcache_1280.db	03/06/2022 14:11	Data Base File	50,176 KB
thumbcache_2560.db	03/06/2022 12:45	Data Base File	91,136 KB
thumbcache_96.db	03/06/2022 09:32	Data Base File	11,264 KB
thumbcache_768.db	02/06/2022 17:18	Data Base File	2,048 KB
thumbcache_48.db	02/06/2022 13:47	Data Base File	3,072 KB
thumbcache_idx.db	02/06/2022 13:36	Data Base File	114 KB
thumbcache_16.db	01/06/2022 20:05	Data Base File	1,024 KB
thumbcache_32.db	01/06/2022 20:05	Data Base File	1,024 KB
thumbcache_256.db	01/06/2022 20:05	Data Base File	1,024 KB
thumbcache_1920.db	01/06/2022 20:05	Data Base File	1 KB
thumbcache_custom_stream.db	01/06/2022 20:05	Data Base File	1 KB
thumbcache_exif.db	01/06/2022 20:05	Data Base File	1,024 KB
thumbcache_sr.db	01/06/2022 20:05	Data Base File	1 KB
thumbcache_wide.db	01/06/2022 20:05	Data Base File	1 KB
thumbcache_wide_alternate.db	01/06/2022 20:05	Data Base File	1 KB

Thumbcache.db (thumbnail database)

- What are they
- Evidentiary value in child pornography cases

28



Thumbcache.db
(thumbnail database)

- What are they
- Evidentiary value in child pornography cases

29

- Thumbcache.db are system files (databases);
  - They store thumbnails for different files (.jpeg; .pdf; .avi etc.);
- Even if the target file was deleted/overwritten, the thumbnail could be found in the thumbcache.db;

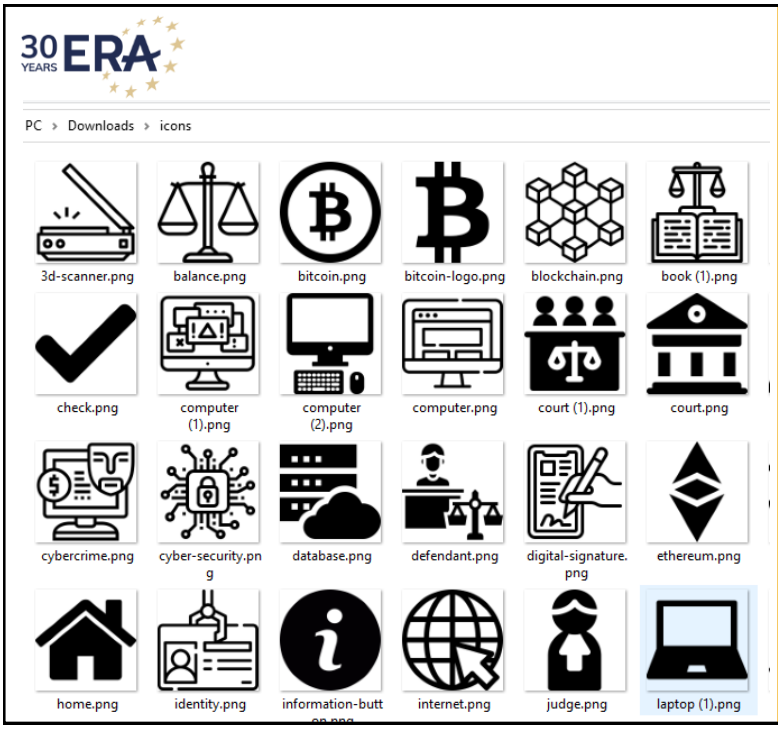
folder with multiple pages, each corresponding to an item in the directory. Viewing a directory icon may trigger thumbnail creation for files within the directory without the user previewing them directly. Additionally, entries are created for files on removable media in the centralised

*S. McKeown, G. Russel, P. Leimich, Fast Forensic Triage Using Centralised Thumbnail Caches on Windows Operating Systems, in Journal of Digital Forensics, Security and Law, vol. 14, no. 3/2019

Thumbcache.db
(thumbnail database)

- What are they
- Evidentiary value in child pornography cases

30



Thumbcache.db
(thumbnail database)

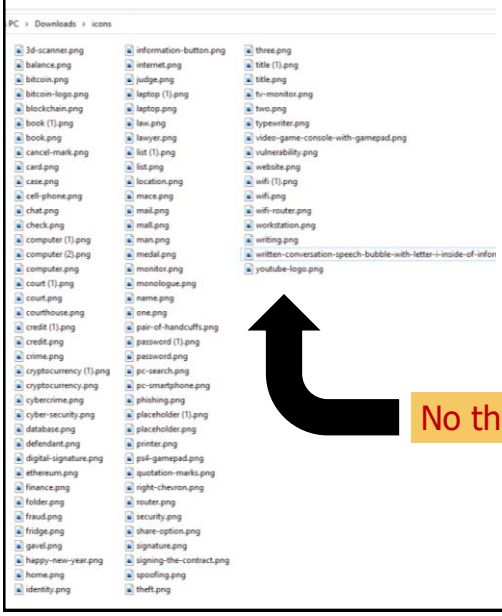
- What are they
- Evidentiary value in child pornography cases

31

Thumbcache.db
(thumbnail database)

- What are they
- Evidentiary value in child pornography cases

32



No thumbnail preview

Thumbcache.db (thumbnail database)

- What are they
- Evidentiary value in child pornography cases

33

- It shows that the computer data was stored on the device
- It does not show that the computer data was accessed (opened) or previewed
- The associated timestamps are for the database, not for the individual files

Thumbcache.db (thumbnail database)

- What are they
- Evidentiary value in child pornography cases

34

- It can show that a computer program was installed or executed from an external device;
  - Relevant for malware attacks;
  - The icon appears in the db even if the program was not executed!
- It can show that a computer program was installed on the computer system and then deleted;
  - Relevant for copyright infringements;
- It can show the path (e.g. USB drive) of the computer program
- We can have a diffferent iconcache.db for each user

Iconcache.db

- What are they
- Evidentiary value

35

Iconcache.db

- What are they
- Evidentiary value

Contents lists available at SciVerse ScienceDirect

Digital Investigation

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

The windows IconCache.db: A resource for forensic artifacts from USB connectable devices

Jan Collie*

Discovery Forensics Ltd, 23 Austin Friars, London EC2N 2QP, UK

36

- **USBStor key**
  - You can find the serial number and other properties of the usb stick or external drive connected to the computer system
  - Relevant for „data theft"
- **Run key**
  - It shows what programs start when the system is booted (e.g. malwares)
- **UserAssist key**
  - You can find information about the most recently used programs
  - + the number of times the programs have been launched
- **Previous wireless connections**
  - Relevant for unauthorized access to a computer system

Windows registry

- Examples
- Evidentiary value

37

Windows registry

- Reading materials

38

SCAN ME

39

THE COLLECTION OF EVIDENCE LOCATED ABROAD AND THE CHALLENGES OF TRANSBORDER ACCESS TO DATA

VILNIUS, 14 JUNE 2022

AVV. FEDERICO DONELLI – PHD
FEDERICO.DONELLI@STUDIOBONATI.NET

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

1

INTRODUCTORY REMARKS

The complexity of the legal framework:

-the first and so far only multilateral treaty which deals with electronic evidence: the Budapest convention of the Council of Europe of 2001;

-the II Protocol of the Budapest Convention;

-the Directive 2014/41/EU on the EIO in criminal Matters;

-Next steps:

- EU Regulation and Directive Proposal on E-Evidence;
- The UN Resolution on a Convention on Cybercrime (74/247 of 27.12.2019 "*Countering the use of information and communication technologies for criminal purposes*");

2

A COMMON DIRECTION….AND ITS REASONS

Enhancing public-private partnerships

Reasons:

1. the relevance of electronic evidence in criminal proceedings;

2. electronic evidence is very often stored on servers and in data centers in foreign countries (cloud);

3. intrinsic characteristics of e-evidence (need for swift retention/collection)

3

DEFINITION(S)

Lack of a common definition for «electronic evidence»

the Budapest convention concepts:
subscriber/traffic/content data

reasons for the distinction

4

OUTLINE

I. Drawbacks of traditional Collection Mechanisms

II. The preference for direct cooperation between LEAs and Service Providers
   A. *De facto*: voluntary disclosure;
   B. Ex cursus: the U.S. Legal framework;
   C. Legal mechanisms enhancing this cooperation:
      1. Article 18 Budapest Convention;
      2. The II Protocol of the Budapest Convention.

5

ALTERNATIVES TO MLA

A. Direct Transborder Access

B. Voluntary Disclosure or Public/private partnership

6

DIRECT TRANSBORDER ACCESS

- Role of consent (case by case/in advance)

- Art. 32 (b) Budapest Convention
  - "A Party may, without the authorisation of another Party… 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."

7

DIRECT TRANSBORDER ACCESS

Limits:

- Data must be located in the territory of a Party;
- The "Lawfully authorized person".

8

VOLUNTARY COOPERATION

What it means: to rely on the willingness of the Provider to cooperate.

Pros: it can be fast and effective

Cons:

- no enforcement;
- no retention period;
- no safeguard for privacy (apart from policies): limitations on content data

9

HURDLES AND TOOLS

-Legal/Procedural hurdles

-Disclosure Policies differ from on provider to another (channel of communication/additional info etc…);

Tools: policies, guidelines, templates for requests

The perspective of the service provider

10

THE U.S. LEGAL FRAMEWORK

- How U.S. Authorities may access data located abroad (Microsoft Case/C.L.O.U.D. Act);
- How and to what extent U.S. based Providers "share" data with foreign authorities;

11

ACCESS BY U.S. LAW ENFORCEMENT AUTHORITIES TO DATA STORED ABROAD

- The Microsoft case (*United States v. Microsoft Corp* - Second Circuit Court of Appeals, 14 July 2016);
- The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 23 March 2018

"A [U.S.-based service provider] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States." (CLOUD Act, § 103(a)(1), adding 18 U.S.C. § 2713)

- Motion to quash or modify the order (18 U.S.C. § 2703 (h)

12

REQUESTS FROM FOREIGN LAW ENFORCEMENT AUTHORITIES FOR ELECTRONIC EVIDENCE STORED IN THE U.S.

- traffic data and subscriber information (voluntary disclosure; 18 U.S.C. § 2702, (c)6)
- When requested to do so, U.S.-based service providers are now allowed to disclose **content** data directly to "qualifying foreign nations", i.e. nations with whom the U.S. has signed an executive data sharing agreement (so-called CLOUD Act agreement)
  - Cloud Act Agreements: restrictions on type of government and type of information

13

REQUESTS FROM FOREIGN LAW ENFORCEMENT AUTHORITIES FOR ELECTRONIC EVIDENCE STORED IN THE U.S.

- After the CLOUD Act
  - Neither the Act nor the agreements it authorizes create a legal obligation for service providers to comply with foreign governments' data demands
  - Concerns raised with respect to privacy, human rights and civil liberties

14

ENHANCING PUBLIC-PRIVATE COOPERATION

- Forerunner: Article 18(1)(b) Budapest Convention

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

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

- Key points:
  - Subscriber information only
  - "offering its services in the territory of the Party"?
  - Data in the person's physical possession or outside the person's physical possession and remotely stored but over which it has control (regardless of where the data is physically located)
- *Belgium v. Yahoo!* (Supreme Court of Belgium, 1 December 2015)

15

THE SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION

1. Implementation of direct cooperation measures (Section 2 – Procedures enhancing direct co-operation with providers and entities in other Parties)

2. MLA instruments as possible enforcement measures in case of non deliverance (Section 3 – Procedures enhancing international co-operation between authorities for the disclosure of stored computer data)

3. Implementation of emergency instruments (artt. 9 and 10)

4. Safeguards (art. 14)

16

SECTION 2 – ENHANCING DIRECT COOPERATION WITH PROVIDERS

Art. 6 – Request for domain name registration information

Art. 7 – Disclosure of subscriber information

These measures do not work just in a domestic perspective, since each Party undetakes the obligation to adopt measures aimed at:

- Empowering its competent Authorities to issue such requests
- Allowing the private entities in its territory to disclose such information in response (in their possession or control)

17

ART. 6 – DOMAIN NAME REGISTRATION

What kind of data ?

What kind of private entity?

Enforcement

18

ART. 7 – DISCLOSURE OF SUBSCRIBER INFORMATION

1. Each Party shall adopt such legislative and other measures as may be necessary to **empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party**, in order to obtain the disclosure of specified, **stored subscriber information in that service provider's possession or control**, where the subscriber information is needed for the issuing Party's **specific criminal investigations or proceedings**.

2. a. Each Party shall adopt such legislative and other measures as may be **necessary for a service provider in its territory to disclose subscriber information in response** to an order under paragraph 1.

19

ART. 7 – DISCLOSURE OF SUBSCRIBER INFORMATION

Key issues/limitations:

- Specific criminal investigation or proceeding;
- it regards subscriber information (definition problem);
- The Authority issuing the order
- Role of the service provider: must be located in the territory (simultaneous notification possible) / obligation on the service provider to consult – possible condition that request be supervised by judicial authority
- Grounds for refusal and enforcement

20

SECTION 3 – ENHANCING INTERNATIONAL COOPERATION BETWEEN AUTHORITIES

Art. 8 (*Giving effect to orders from another Party for expedited production of subscriber information and traffic data*)

1. Each Party shall adopt such legislative and other measures as may be necessary to **empower its competent authorities to issue an order to be submitted as part of a request** to another Party for the purpose of compelling a **service provider in the requested Party's territory** to produce specified and stored

a. **subscriber information**, and

b. **traffic data**

in that service provider's **possession or control** which is needed for the Party's specific criminal investigations or proceedings.

2. Each Party shall adopt such legislative and other measures as may be necessary to **give effect to an order under paragraph 1** submitted by a requesting Party.

21

SECTION 3 – ENHANCING INTERNATIONAL COOPERATION BETWEEN AUTHORITIES

Key issues:

-purpose;

-scope;

-legal tools (the «order» and «giving effect to it»);

-transmission and public-private interaction;

-time;

-enforcement.

22

ART. 9 AND 10 – EMERGENCY DISCLOSURE

Art. 9 – Expedited disclosure of stored computer data in an emergency (without MLA Request)

Art. 10 – Emergency MLA (section 4 – Procedures pertaining to emergency mutual assistance)

Scope:

- Also content data
- Definition of emergency (art. 3, II Protocol): an "emergency" means a situation in which there is a significant and imminent risk to the life or safety of any natural person;

23

THANK YOU FOR YOUR ATTENTION!

24

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

University of Antwerp
Faculty of Law

The (limited) effectiveness of MLA instruments in the digital age

Prof. dr. Joachim Meese
associate professor
attorney

1

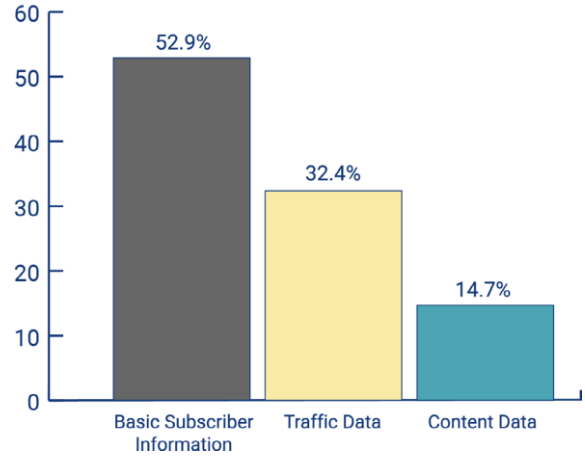
most common types of e-evidence

- **basic subscriber information**
  - e.g. name, e-mail, phone number, …
- **traffic data**
  - e.g. connection logs, number of messages, …
- **content data**
  - e.g. photos, content of messages or e-mails, files, …

2

most common types of e-evidence

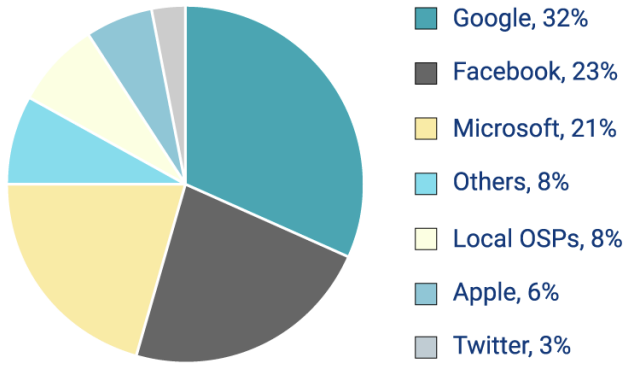
- most often needed type of e-evidence from foreign authorities or online service providers in 2019:



3

most common types of e-evidence

- three most contacted online service providers in 2019:



4

characteristics of e-evidence

- **volatile, can easily and quickly be deleted**
- **cross-border**
  - according the Commission 85% of criminal investigations require electronic evidence
  - approx. 2/3 of electronic evidence is located in another State (both within and outside the EU)
- **necessity for quick intervention**
- **hard to locate and access evidence**
  - e.g. in cases where the origin of cyber attacks or location of e-evidence is not (yet) known
  - data redundancy

dealing with e-evidence

- **cloud-stored data: what about jurisdiction?**
  - possible theories:
    - criminal event theory (territorial)
    - criminal instrument theory (territorial)
    - direct consequence theory (extra-territorial)
    - nationality principle theory (extra-territorial)

dealing with e-evidence

- **key aspects:**
  - ensuring authenticity of digital data
  - chain of custody
    - proper and detailed documentation of access to data, its storage, copying and analysis (without changing the data)
    - analysis and further work with digital data is only done with a copy, not the original set of data
    - proper documentation of the police staff that is involved and the IT forensic software that is being used
  - see ACPO Good Practice Guide for Digital Evidence

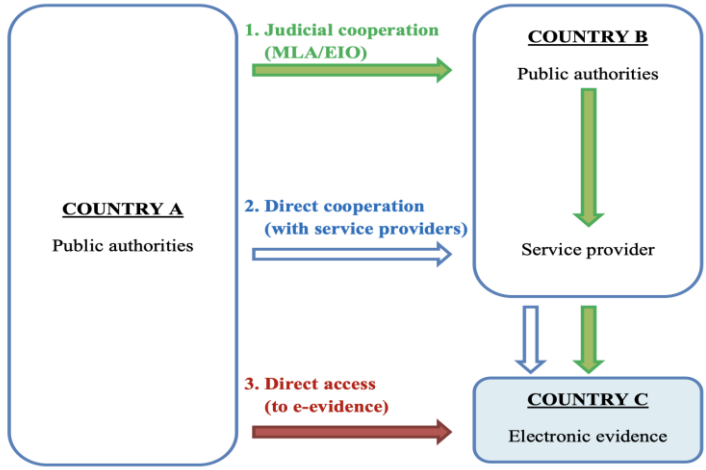
https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

dealing with e-evidence

- **common procedures for recognising & handling e-evidence**
  - in most European member States: no specific regulations
    - e.g. Belgium
  - therefore:
    - general principles of dealing with analogue evidence also apply to digital/electronic evidence
    - (soft) regulations within different authorities (e.g. police, federal authorities like the Belgian FCCU)
    - best practices and efforts to certificate certain IT forensic software
    - legislation on the international/European level

cross-border access to evidence

- **possible scenarios:**

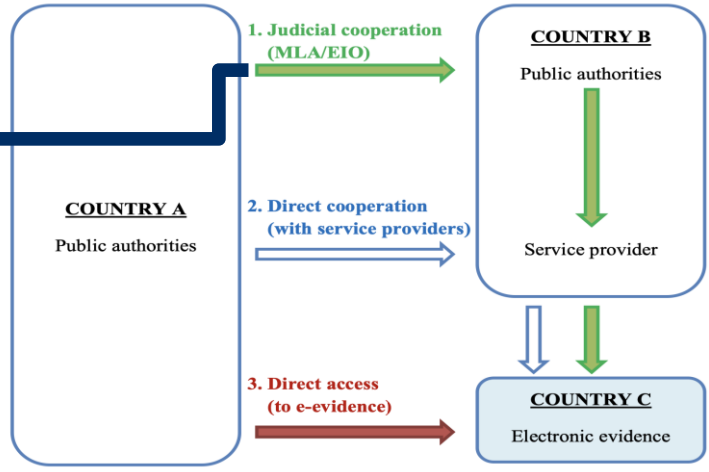


9

cross-border access to evidence

- **possible scenarios:**

✓ within EU: EIOD
✓ outside EU: international agreements
- Budapest Convention on cybercrime
  - 2nd additional protocol can be signed by MS in the interest of the EU (Council decision of 5 April 2022)
    - ✓ improve international cooperation
    - ✓ enhance direct cooperation
    - ✓ emergency mutual assistance
- bilateral agreements concluded by
  - the EU (e.g. the agreement with the US of 23 October 2009)
  - the member States (most frequently with the US, Canada or Australia)



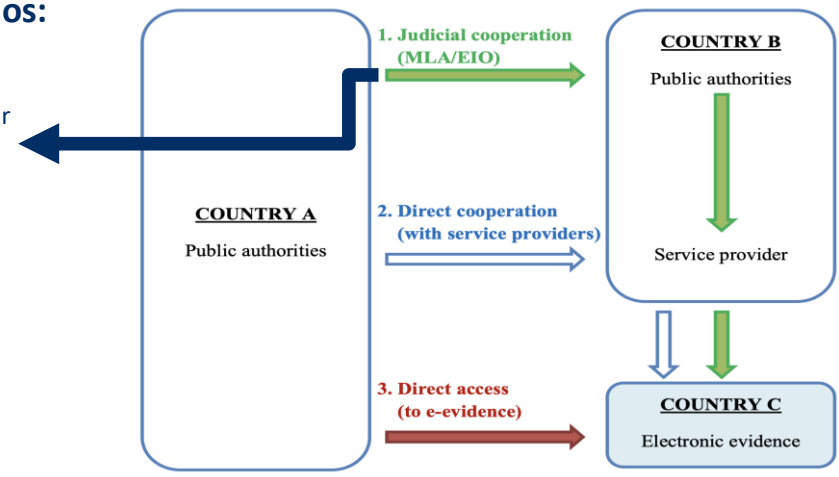
10

cross-border access to evidence

- **possible scenarios:**

number of requests per year on e-evidence:

- ✓ between EU member States: 13.000
- ✓ EU MS to US: 1.300

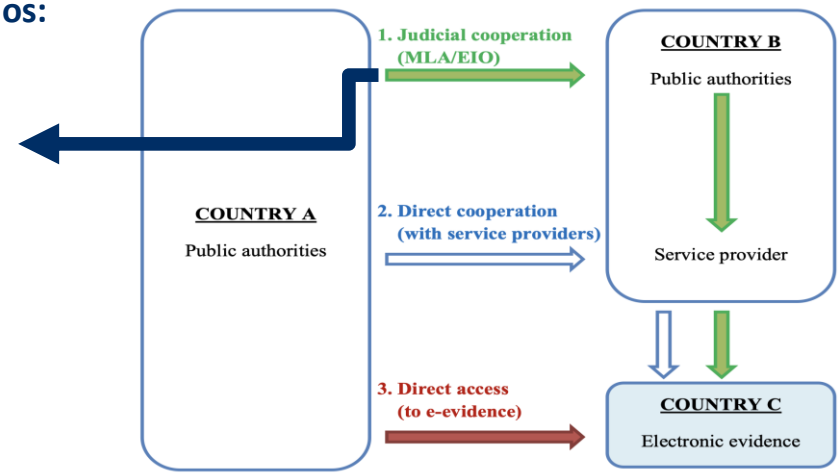


11

cross-border access to evidence

- **possible scenarios:**

- ✓ MLA challenges
  - hard to get a timely response to a request
  - too much formalities
  - too complicated and technical to use

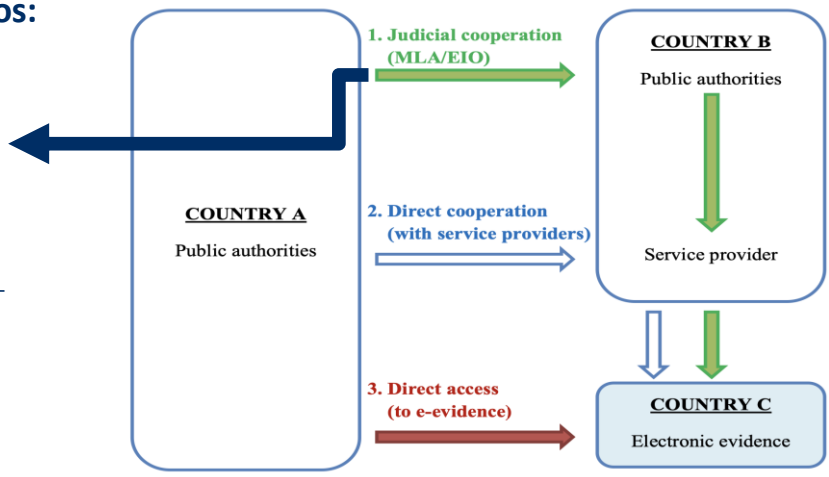


12

cross-border access to evidence

- **possible scenarios:**

✓ EIOD challenges
- Ireland, Denmark and UK are not bound
- too slow for e-evidence
- too formalistic for e-evidence
- not adapted to complex e-evidence situations
- high cost and capacity requirements
- legal impediments



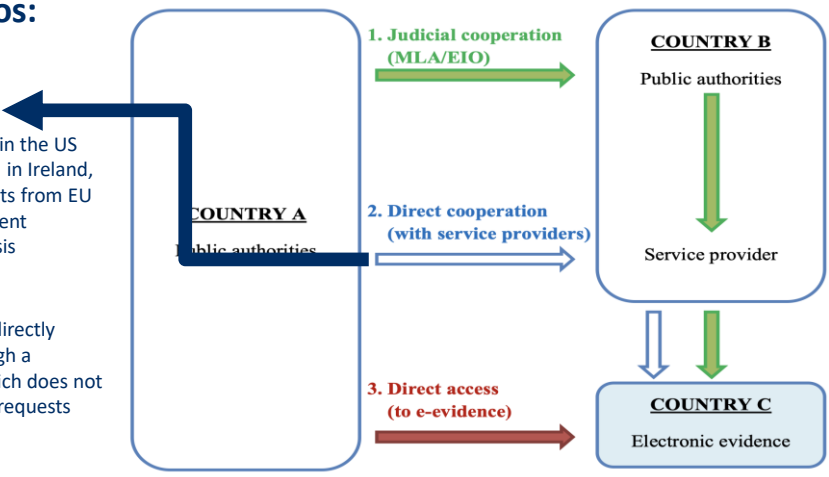
13

cross-border access to evidence

- **possible scenarios:**

✓ non-content data
- service providers established in the US and, to a more limited extent, in Ireland, which reply directly to requests from EU member States law enforcement authorities on a voluntary basis

✓ WHOIS data
- service providers make data directly available to authorities through a centralised search system which does not rely on individually reviewed requests

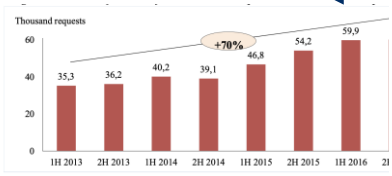


14

cross-border access to evidence

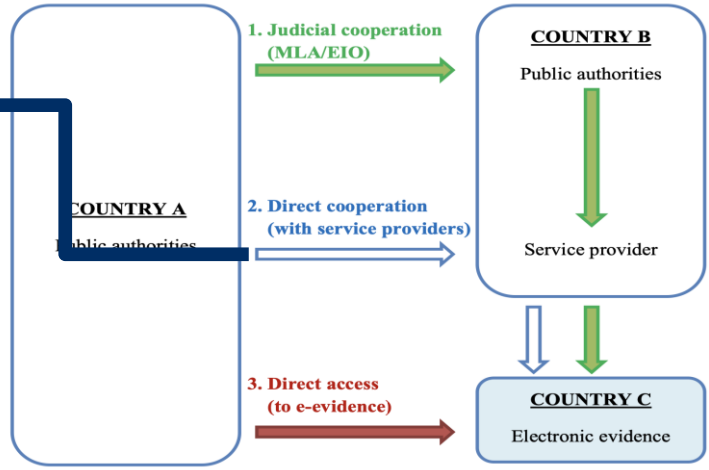
- **possible scenarios:**

numbers:



→ in 2018, 3 member States account for > 75% of all requests from the entire EU
- Germany: 35.271
- UK: 28.598
- France: 27.268

→ Google & Facebook: 70% of total requests

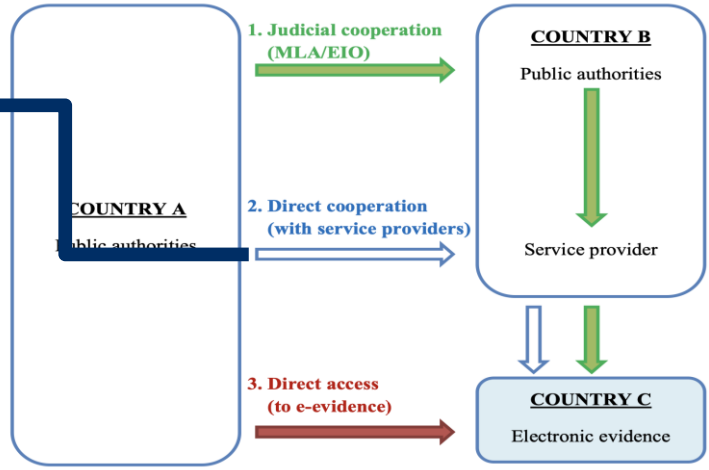


15

cross-border access to evidence

- **possible scenarios:**

✓ challenges
- can be unreliable
- can take too long
- only possible with a limited number of service providers
- providers all apply different policies
- not transparent
- lacks accountability in case of non-compliance
  - see, however the Belgian case of YAHOO! (Cass. 1 December 2015, P.13.2082.N)



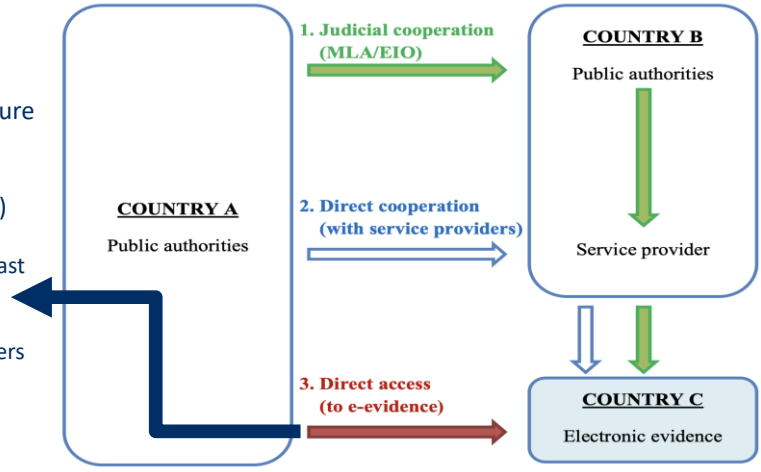
16

cross-border access to evidence

- **possible scenarios:**

✓ extended search (following seizure of a device)
✓ remote search (following lawful acquisition of login information)

→ possible under national law of at least 20 member States
→ this tool becomes more relevant
  - data are regularly stored on servers in a different location
  - in case of loss of knowledge of location of data (e.g. Darknet)

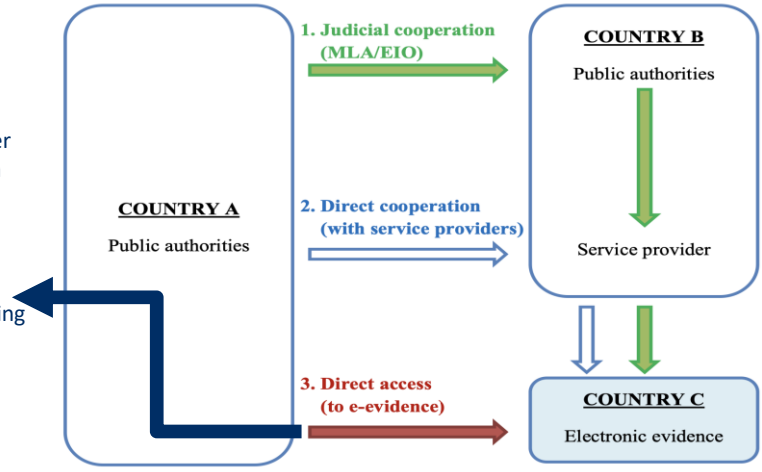


17

cross-border access to evidence

- **possible scenarios:**

✓ challenges
  - different approaches by member States to direct access & to data storage location
  - risk of losing data
    - ✓data can easily and swiftly be deleted from another device
    - ✓data can be lost when gathering and moving it



18

cross-border access to evidence: what about EPO?

- **EPO (not into force yet)**
  - what: legal framework laying down the rules under which an authority of a Member State may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data
    - EPdO: European Production Order (<-> EPOC)
    - EPsO: European Preservation Order (<-> EPOC-PR)
  - title: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters
  - background: driven by the fight against terrorism
    - establishing security is one of top policy priorities of the EU
    - an instrument for transnational access to e-evidence in the EU is a pressing issue

cross-border access to evidence: what about EPO?

- **EPO**
  - texts & sources
    - original Commission proposal (17 April 2018)
      - https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2018/0225/COM_COM(2018)0225_EN.pdf
    - the Council's general approach (11 Juni 2019)
      - https://data.consilium.europa.eu/doc/document/ST-10206-2019-INIT/en/pdf
    - Report Committee on Civil Liberties, Justice and Home Affair (11 December 2020)
      - https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html
    - Report from the Commission to the European Parliament and the Council (20 July 2021)
      - https://data.consilium.europa.eu/doc/document/ST-11007-2021-INIT/en/pdf
      - launch of EU-US negotiations to facilitate access to electronic evidence: 19 July 2021
    - Draft regulation:certain issues (26 August 2021)
      - https://db.eurocrim.org/db/en/doc/3646.pdf

cross-border access to evidence: what about EPO?

- **EPO**
  - texts & sources
    - State of play and possible ways forward (16 September 2021)
      - https://www.statewatch.org/media/2739/eu-council-e-evidence-regulation-state-of-play-11681-21.pdf
      - Report of 20 December 2021: https://www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html
      - update of 23 February 2022: https://www.statewatch.org/media/3175/eu-council-e-evidence-4-col-doc-regulation-6487-22.pdf
      - letter of EP's rapporteur (16 February 2022): https://www.statewatch.org/media/3174/eu-council-e-evidence-mep-rapporteur-letter-6323-22.pdf
    - also important: 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
      - https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2018:226:FIN
      - general approach: https://data.consilium.europa.eu/doc/document/ST-7348-2019-INIT/EN/pdf

Comparative scheme: key characteristics

MLA

- traditional instrument of international cooperation
- all kinds of investigative measures
- important in the relationship with third States, mainly with the USA
- complex, lots of formalities, takes time

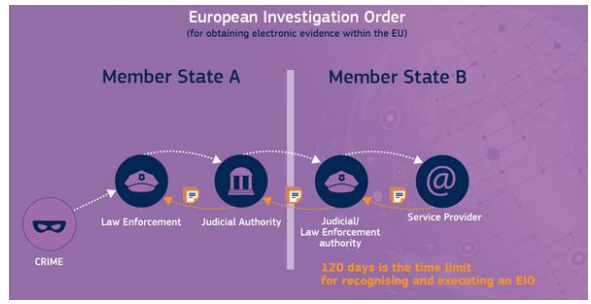
EIOD

- all kinds of investigative measures (except in the framework of JIT)
- inspired by mutual recognition
- execution by domestic authorities or by third parties
- in theory within 120 days
- Directive

EPO

- only for electronic information
- restricted to criminal proceedings
- directly addressed to service provider and to executing authority
- some orders can be issued for all criminal offences and for most types of data stored
- location of data is not relevant
- a new type of cooperation instrument based on advanced form of mutual trust
- (extraordinary?) simplification of procedure
- Regulation (no transposition!)

Comparative scheme: visual representation



23

Thank you!

@ joachim.meese@uantwerp.be
www.linkedin.com/in/joachimmeese/
@JoachimMeese

24

Digital investigations and electronic evidence in court: a new evidentiary frontier for prosecutors - Wednesday 15 June 2022 (09:30 - 10:15).

mr. M.J.M. (Marc) van der Ham - m.van.der.ham@om.nl
Dep. Team Lead at the Dutch Public Prosecution Service & PhD-candidate at Leiden University

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES
FOCUS ON INTERNET SEARCHES FOR EU LEGAL PRACTITIONERS Vilnius, 14-15 June 2022

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

1

Disclaimer: This presentation and lecture is not an official position of the Dutch Public Prosecution Service and only represents the personal views and interpretations of the speaker.

2

Marc van der Ham is Deputy Team Lead of the Policy Strategy Team in the **National Office of the Dutch Prosecution Service** and a Senior Legal Advisor in its High Tech Investigations Unit. Before joining the prosecution service in 2017, he worked as a legal advisor at Google EMEA and in the European Parliament.

Since August 2020, Marc has been an external PhD candidate at the **eLaw, the Center for Law and Digital Technologies, at Leiden University**. His research explores legal assistance obligations for IT infrastructure companies in criminal investigations of disruptive cybercrime.

Marc graduated in European Law and Philosophy of Law from Leiden University. Follow Marc on Twitter @marcvanderham.

3

Agenda

- Challenges posed by websites, social networks and cloud environments
- The collection and processing of data in criminal investigations
- Admissibility of evidence in court
- Equality of arms
- Q&A

4

Challenges posed by websites, social networks and cloud environments

- ➢ Boundary between the police's own competence and the role of the public prosecutor
  - ➢ Criminal investigations, open - vs. publicly accessible sources (> search engine, dark web)
  - ➢ Effective control, security measures, virtual agents (≠ illegal access, ≠ infiltration)
  - ➢ Level of infringement: substantive criteria - to be determined in advance (crawlers)
  - ➢ Specific goals vs. structurally and systematic monitoring / special investigatory powers
- ➢ Determining the correct addressee of an order and its substantive requirements
  - ➢ Where is the company incorporated?
  - ➢ Hosters, resellers and jurisdictional issues (familiar problem?)
  - ➢ Practical issues and governance on the side of police and public prosecutor

5

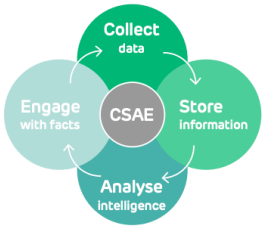
The collection and processing of data in criminal investigations

- ➢ Voluntary disclosure, open source, execution of a court order and MLA's
- ➢ Mutual legal assistance and the principle of trust in international judicial cooperation
  - ○ The principles of sovereignty and purpose limitation
  - ○ NL: execution of outgoing MLA can be done in ways not allowed in NL (except..)
- ➢ Public-private cooperation in criminal investigations
  - ○ Data protection law obligations (Electronic Crimes Task Force, Cyber Threat Intel)
  - ○ Article 26 GDPR on joint controllers
- ➢ Legal hacking
  - ○ The use of technical (commercial) tooling and their screening

6

Admissibility of evidence in court

- Collect, Store, Analyze, Engage (the CSAE-model*) and a prosecutor's role
  - The impact of EU data protection law (GDPR & LED)
- The use of data in criminal proceedings
  - Quality, authenticity, integrity, interpretability, explainability
  - Sensors, pedometer, supporting evidence
  - Forensic readiness
- Principles of (Dutch) evidence law
  - Discretion of judge to select and appreciate, all available material, limited motivation
  - Substantive truth, the offence charged is proven it the judge is 'convinced'
  - Reliability and legitimacy



(*) Towards Data Scientific Investigations: A Comprehensive Data Science Framework and Case Study for Investigating Organized Crime and Serving the Public Interest Prepared by Erik van de Sandt *†‡§, Arthur van Bunningen† , Jarmo van Lenthe† , John Fokker¶

7


deVolkskrant

RECONSTRUCTIE MOORD OP DE BÜTERWEI

Hoe Google-data in een moordzaak leidden naar de echtgenote

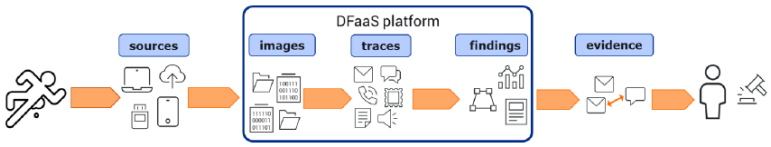
1. Text messages
2. Search history
3. Camera images
4. Location history
5. Battery status
6. High precision / sensor
7. Throttling mode
8. Security cameras

Will the Supreme Court annul the decision?

8

Equality of arms

- Hansken and Digital Forensics as a Service (DFaaS): insightful, accessible, searchable
  - Overwhelming amount of data, fast, accessible beyond experts,
  - Academy, Community to share knowledge/software, cooperate, build plugins, open platform, legal / forensic / security requirements,
- Access to data and the right to a fair trial (Sigurdur Einarsson and others vs. Iceland)
  - Selection of complete data set can be made (can the defence be involved?)
  - Should access to a sophisticated search engine be provided?
  - Sufficient time and opportunity by the defence to analyze the evidence
- Recent Encrochat case law (Title V & IV CCP, sharing of information, additional judgment by investigatory judge, Prokuratuur Case C-746/18, French and Dutch cooperation in JIT).



9

Q&A

10

Discussion: Legal assistance obligations for ‘IT infrastructure companies’ in criminal investigations of ‘disruptive cybercrime’

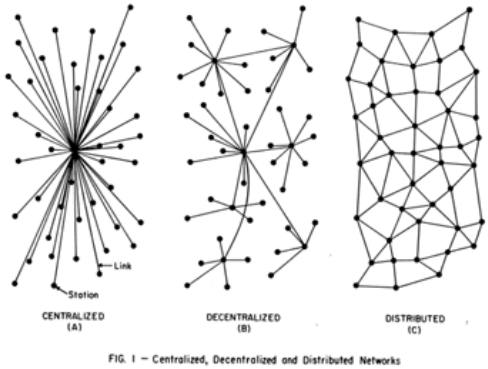


FIG. 1 — Centralized, Decentralized and Distributed Networks

Source: Introduction to Distributed Communications Networks, Paul Baran

Cybercrime can have disruptive effects on society. However, perpetrators of this type of cybercrime are rarely prosecuted. Often because they enjoy protection from foreign governments. Also because law enforcement has little information about these crimes or no access to compromised networks. This situation undermines the trust of citizens in society, digital technologies and the rule of law. To end impunity for disruptive cybercrime, should companies with a key position in the Internet infrastructure be obliged to assist in criminal investigations?

11

WKB lawyers

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

e-Evidence and online investigation results in court

A practitioner's perspective

Aleksandra Stępniewska, advocate, WKB

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

Vilnius, 14-15 June 2022

1

WKB lawyers

e-Evidence and online investigation results in criminal proceedings

Lawyer vs. e-evidence

I. WHAT TYPE OF E-EVIDENCE A LAWYER CAN HAVE ACCESS TO?

II. WHY AND HOW AN E-EVIDENCE CAN BE USEFUL TO A LAWYER?

III. CREDIBILTY OF THE E-EVIDENCE AT TRIAL

2

WKB lawyers

WHAT TYPE OF E-EVIDENCE A LAWYER CAN HAVE ACCESS TO?

3

WKB lawyers

WHAT TYPE OF E-EVIDENCE A LAWYER CAN HAVE ACCESS TO?

What is an electronic evidence?

“Electronic 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.”

ELECTRONIC EVIDENCE IN CIVIL AND ADMINISTRATIVE PROCEEDINGS
Guidelines adopted by the Committee of Ministers of the Council of Europe on 30 January 2019

~any representation of facts, information, or concepts in a form suitable for processing in a computer system

4

WHAT TYPE OF E-EVIDENCE A LAWYER CAN HAVE ACCESS TO?

Open sources

- Websites
- Websites with archived websites
- Snapshots
- Social media (fb, Twitter, Instagram)
- Tools for reading the headers
- Online toolkit
- Google maps
- Street review
- Darknet – sources of leaks

Covert sources

- E-mails (including headers)
- Pictures
- Sms
- Voice messages
- Video, CTTV records
- GPS data
- Public records
- Public information

Hacking methods in order to gather evidence → national law considerations
False accounts in order to obtain IP of the computer

5

BUT DON'T GO TO DEEP

6

WHAT TYPE OF E-EVIDENCE A LAWYER CAN HAVE ACCESS TO?

Online toolkit:

- **Wayback machine https://web.archive.org/ → archival versions of websites**
- **Built With https://builtwith.com/ → i.a. domains connected to a domain at the collimator of suspicion**
- **Statscrop https://www.statscrop.com/ → Free Online Website Analyzer**
- **Messageheader https://toolbox.googleapps.com/apps/messageheader/ → analysis of headers of e-mails**
- **Ripe Database https://www.ripe.net/manage-ips-and-asns/db → contains registration information for networks, i.a. identification of a provider of services to a person using a specific IP address**

7

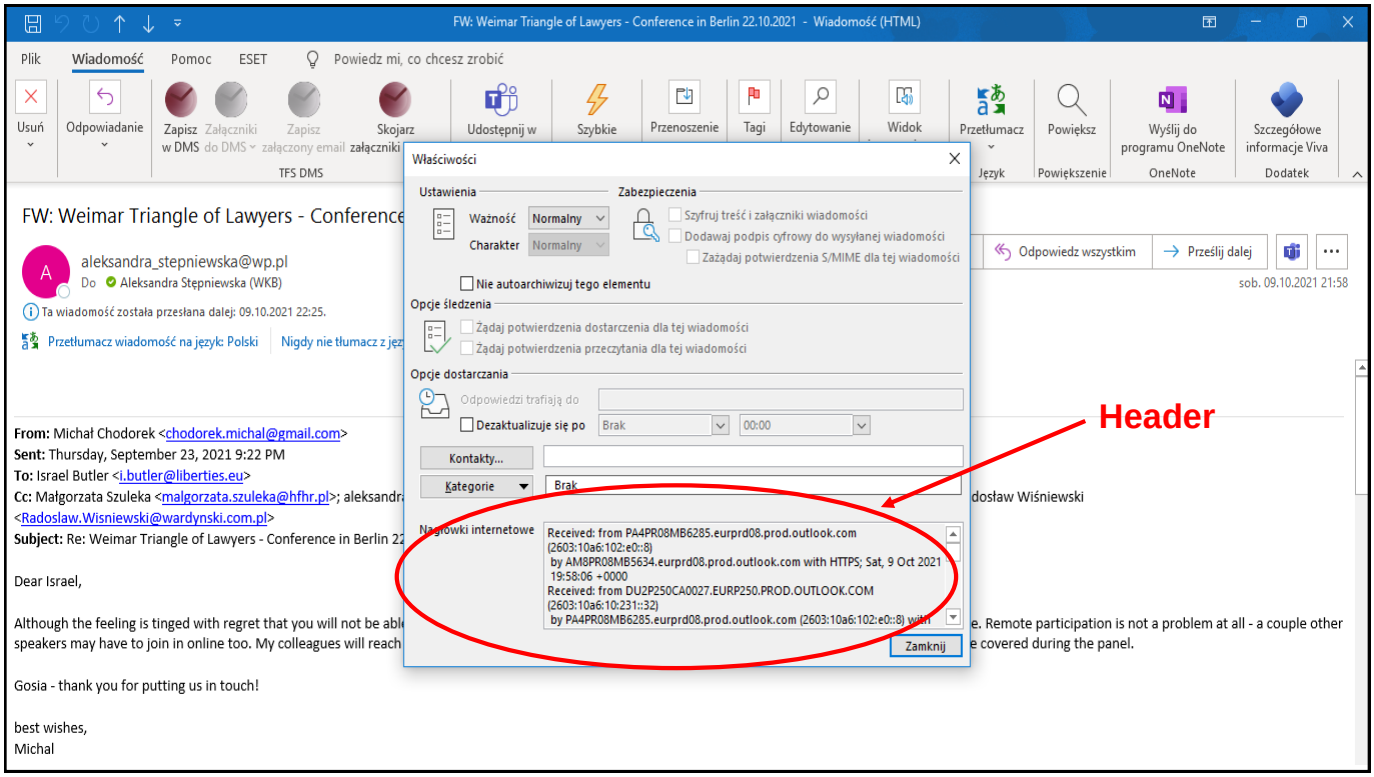
WHAT TYPE OF E-EVIDENCE A LAWYER CAN HAVE ACCESS TO?

Messageheader

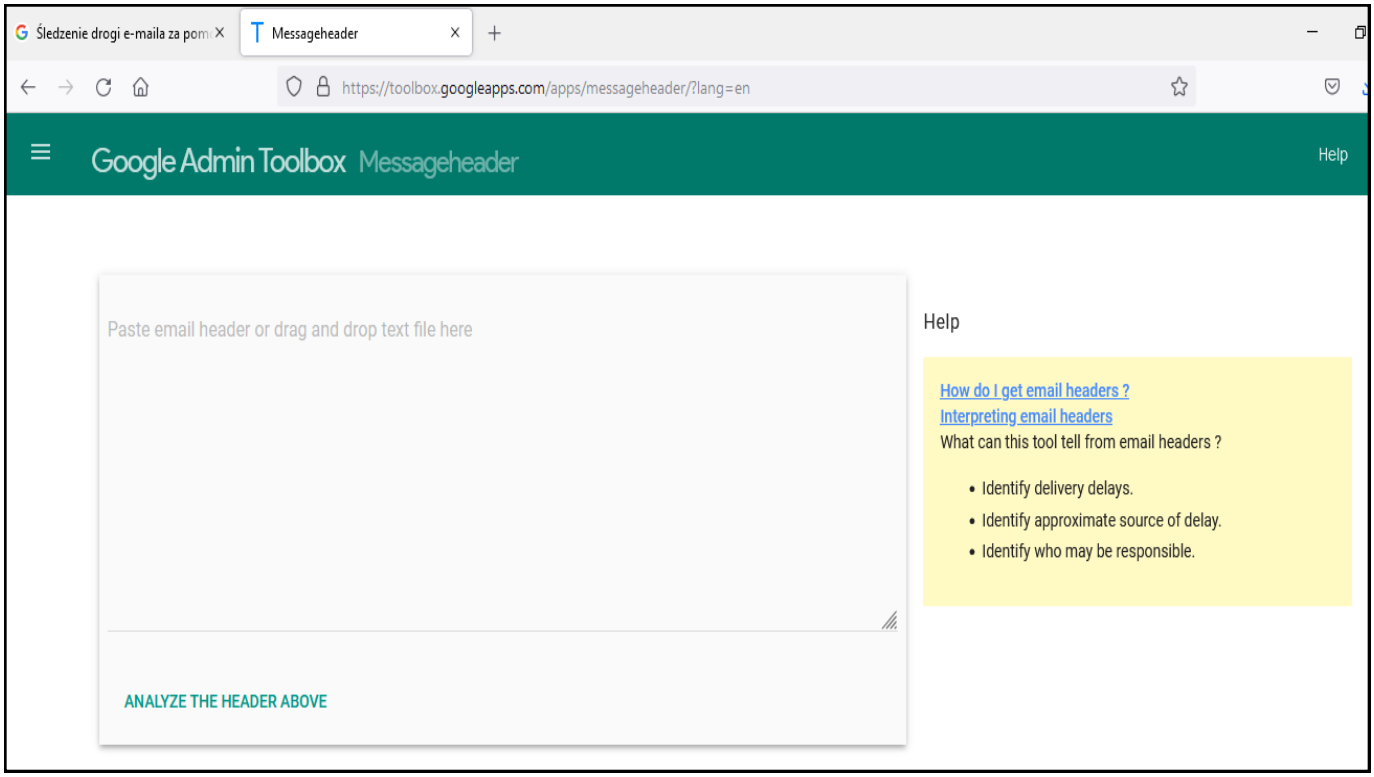
https://toolbox.googleapps.com/apps/messageheader/

analysis of an e-mail header

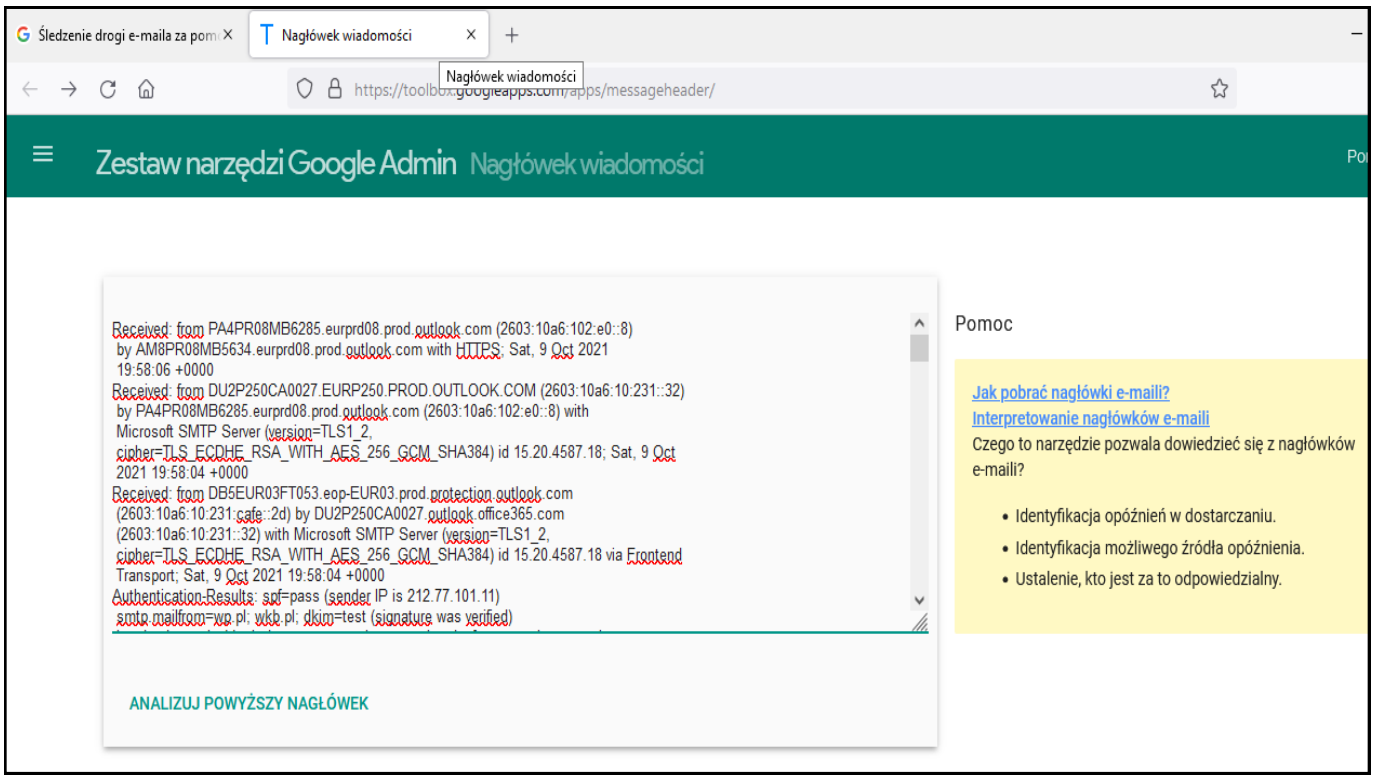
8


FW: Weimar Triangle of Lawyers - Conference in Berlin 22.10.2021 - Wiadomość (HTML)
Właściwości
Header
From: Michał Chodorek <chodorek.michal@gmail.com>
Sent: Thursday, September 23, 2021 9:22 PM
To: Israel Butler <i.butler@liberties.eu>
Cc: Małgorzata Szuleka <malgorzata.szuleka@hfhr.pl>; aleksandra
<Radoslaw.Wisniewski@wardynski.com.pl>
Subject: Re: Weimar Triangle of Lawyers - Conference in Berlin 22
Dear Israel,
Although the feeling is tinged with regret that you will not be abl
speakers may have to join in online too. My colleagues will reach
Gosia - thank you for putting us in touch!
best wishes,
Michal

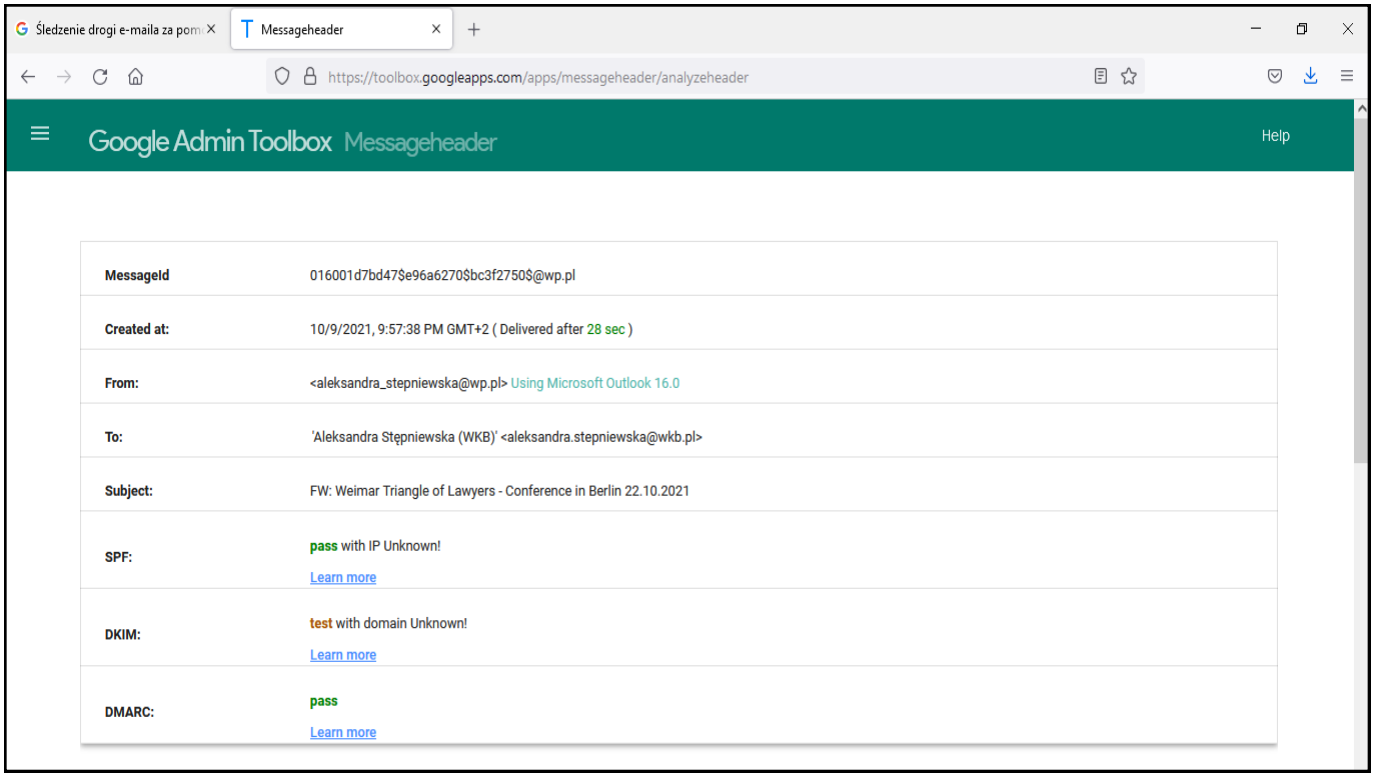
9


Messageheader
https://toolbox.googleapps.com/apps/messageheader/?lang=en
Google Admin Toolbox Messageheader
Help
Paste email header or drag and drop text file here
ANALYZE THE HEADER ABOVE
Help
How do I get email headers ?
Interpreting email headers
What can this tool tell from email headers ?
• Identify delivery delays.
• Identify approximate source of delay.
• Identify who may be responsible.

10


Śledzenie drogi e-maila za pom
Nagłówek wiadomości
Nagłówek wiadomości
https://toolbox.googleapps.com/apps/messageheader/
Zestaw narzędzi Google Admin Nagłówek wiadomości
Received: from PA4PR08MB6285.eurprd08.prod.outlook.com (2603:10a6:102:e0::8)
by AM8PR08MB5634.eurprd08.prod.outlook.com with HTTPS; Sat, 9 Oct 2021
19:58:06 +0000
Received: from DU2P250CA0027.EURP250.PROD.OUTLOOK.COM (2603:10a6:10:231::32)
by PA4PR08MB6285.eurprd08.prod.outlook.com (2603:10a6:102:e0::8) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4587.18; Sat, 9 Oct
2021 19:58:04 +0000
Received: from DB5EUR03FT053.eop-EUR03.prod.protection.outlook.com
(2603:10a6:10:231:cafe::2d) by DU2P250CA0027.outlook.office365.com
(2603:10a6:10:231::32) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4587.18 via Frontend
Transport; Sat, 9 Oct 2021 19:58:04 +0000
Authentication-Results: spf=pass (sender IP is 212.77.101.11)
smtp.mailfrom=wp.pl; wkb.pl; dkim=test (signature was verified)
ANALIZUJ POWYŻSZY NAGŁÓWEK
Pomoc
Jak pobrać nagłówki e-maili?
Interpretowanie nagłówków e-maili
Czego to narzędzie pozwala dowiedzieć się z nagłówków e-maili?
Identyfikacja opóźnień w dostarczaniu.
Identyfikacja możliwego źródła opóźnienia.
Ustalenie, kto jest za to odpowiedzialny.

11


Śledzenie drogi e-maila za pom
Messageheader
https://toolbox.googleapps.com/apps/messageheader/analyzeheader
Google Admin Toolbox Messageheader
Help
MessageId 016001d7bd47$e96a6270$bc3f2750$@wp.pl
Created at: 10/9/2021, 9:57:38 PM GMT+2 (Delivered after 28 sec)
From: <aleksandra_stepniewska@wp.pl> Using Microsoft Outlook 16.0
To: 'Aleksandra Stępniewska (WKB)' <aleksandra.stepniewska@wkb.pl>
Subject: FW: Weimar Triangle of Lawyers - Conference in Berlin 22.10.2021
SPF: pass with IP Unknown!
Learn more
DKIM: test with domain Unknown!
Learn more
DMARC: pass
Learn more

12

WKB lawyers

WHAT TYPE OF E-EVIDENCE A LAWYER CAN HAVE ACCESS TO?

Lawyer vs. e-evidence

BUT WHAT IN FACT IS IMPORTANT?

Certainly the IP address

13

WKB lawyers

WHAT TYPE OF E-EVIDENCE A LAWYER CAN HAVE ACCESS TO?

- Money on a bank account – can it be an evidence ?
- Wire fraud cases
- Freezing the money for 3, 6, 12 months
- And what next ?
- Seizure to secure the execution of the judgement or as an evidence
- Problem of 3 D

14

WKB lawyers

WHY AND HOW AN E-EVIDENCE CAN BE USEFUL TO A LAWYER?

15

WKB lawyers

WHY AND HOW AN E-EVIDENCE CAN BE USEFUL TO A LAWYER?

Lawyer vs. e-evidence

- For the defence → i.a. undermining conclusions of algorithms
- For the aggrieved party → substantiation of a probable case while filing a notification of a suspected offence
- Internal investigations as a result of a report made within an organisation → a second revolution came i.e. the Whistle-blowers Protection Directive

16

WKB lawyers

WHY AND HOW AN E-EVIDENCE CAN BE USEFUL TO A LAWYER?

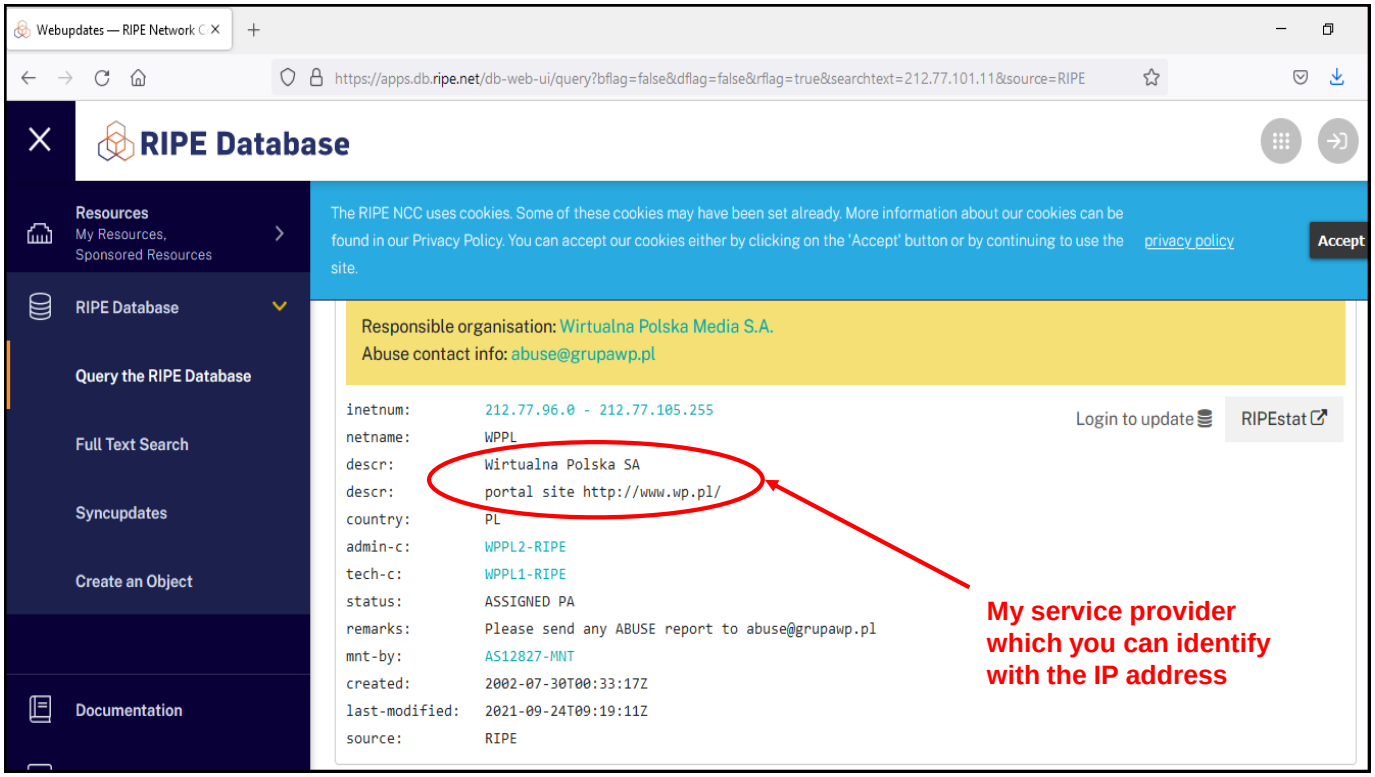
Lawyer vs. e-evidence

- **Wire transfer fraud**
  - **Analysis of headers → e-mail mirroring**
    - aleksandra.stepniewska@wkb.pl
    - aleksandra.stepniewska@wkb.pl
  - **Analysis of the IP**
  - **Results of the IT investigation**

ALEKSANDRA.STEPNIEWSKA@WKB.PL

AIEKSANDRA.STEPNIEWSKA@WKB.PL

17



18

WKB lawyers

- Where do you live?
- Who you are married to?
- Where do you work?
- For how long you are with FB?
- Your posts

19

WKB lawyers

ADMISSIBILITY AND CREDIBILTY OF THE E-EVIDENCE AT TRIAL

20

WKB lawyers

ADMISSIBILITY AND CREDIBILTY OF THE E-EVIDENCE AT TRIAL

Lawyer vs. e-evidence

- Admissibility
  1. Relevancy → evidence has a tendency to make a fact more or less probable than it would be without the evidence
  2. Reliability → e-evidence must be authentic and identified as evidence
  3. Not unfairly prejudicial → there will be no harm resulting from admission of the evidence
  4. Legalilty

21

WKB lawyers

ADMISSIBILITY AND CREDIBILTY OF THE E-EVIDENCE AT TRIAL

Lawyer vs. e-evidence

- Seizure and storage → crucial for e-evidence authenticity
  - Forensic → private sector (sometimes also serves enforcement authorities)
  - Custody chain
  - # function
  - Cloud
  - Mirror image
  - Notaries

22

CREDIBILTY OF THE E-EVIDENCE AT TRIAL

Lawyer vs. e-evidence

- Seizure and storage of e-evidence authenticity → best practicies
  - Competence
  - Documenting
  - Apropriate storage (f.ex. no light exposure)
  - Data integrity
  - Audit trail – the same result

23

ADMISSIBILITY AND CREDIBILTY OF THE E-EVIDENCE AT TRIAL

Lawyer vs. e-evidence

- Gordian knot of e-evidence credibility
  - What can be the probatory power of an e-evidence
  - Presumption of reliability
  - It cannot be a queen of evidence
- Presentation → contradictory discussion
  - Why this e-evidence
  - Logic and code of seizure and storage → metadata
  - Evidence was not a subject to an alteration
  - Language skills

24

WKB lawyers

PROBLEMS

Lawyer vs. e-evidence

I. Social media – everyone can write everything
II. Reliability of e-evidence produced by the lawyer vs. the effectiveness of the Justice
III. What can be the use of an e-evidence or an intelligence investigation gathered or made by a lawyer
IV. Technical knowledge
V. Should electronic evidence be evaluated in the same way as other types of evidence

25

ALEKSANDRA STĘPNIEWSKA
advocate, *counsel*

aleksandra.stepniewska@wkb.pl
+48 509 067 919

WKB Wierciński, Kwieciński, Baehr sp. j.
Warszawa Plac Małachowskiego 2 • 00-066 Warszawa • Tel. +48 22 201 00 00
Poznań ul. Paderewskiego 7 • 61-770 Poznań • Tel. +48 61 855 32 20

office@wkb.pl
www.wkb.pl

26