ERA
european.law

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

ONLINE INVESTIGATIONS: WEBSITES AND SOCIAL MEDIA

Prague, 18-19 October 2021

UP GRADE
YOUR LEGAL EXPERTISE

Criminal Law

Professional Training (CPD) www.era.int

Speakers and chairs

Patricia Ayodeji, Dual-Qualified Solicitor for England & Wales, Lawyer (Abogado) for Spain, Barcelona

Steven David Brown, International Cybercrime Consultant, Vienna

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

Muthupandi Ganesan, Barrister at Law & Partner, Aliant Law, London

Petar Majic, Digital Forensic Consultant, INsig2, Zagreb

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

Dennis Pielken, Lecturer, Cybercrime & Digital Investigations, Rhineland-Palatinate Police University

Claudia Pina, Investigating Judge (JLD), SNE, Operations Department – Casework Unit; Coordinator of the European Judicial Cybercrime Network (EJCN) Support Team, The Hague

John Van Krieken, Judge, Court of Appeal, Tilburg

Renata Vystrčilová, Head of Department, Czech Judicial Academy, Kroměříž

Pavel Zeman, Prosecutor, Supreme Public Prosecutor´s Office, Brno

Key topics

- Online investigations on websites
- Investigating social media (open and covert)
- Demonstration of a forensic tool
- e-Evidence and the admissibility test

Language
English

Event number
321DT34f

Organisers
ERA (Laviero Buono) in cooperation with the Czech Judicial Academy

JUSTIČNÍ AKADEMIE

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

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

Monday, 18 October 2021

08:30 Arrival and registration of participants

09:00 **Welcome and introduction to the programme**
Renata Vystrčilová & Laviero Buono

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

Chair: Laviero Buono

09:15 **The Internet: More than an IoTa of evidence**
- More than the WWW (a brief introduction to the Internet)
- Internet history and the cache
- Browser profiling
- Evidence and the Internet of things (Iot)
- Sources and resources
- Kept in the Dork (ways to focus your search strategy)
- Social media: the publisher -v- platform debate

Steven David Brown

10:15 Discussion

10:30 Break

Chair: Joachim Meese

11:00 **Open source tools, computer forensics in the "Cloud"**
- Encryption
- Reverse image search
- How to review a webpage or site that is offline
- Physical and logical acquisition of data
- Cloud providers and replicated data on websites and social media

Petar Majic

11:45 **Open Source Intelligence and social media: finding the needle in Facebook, Instagram and others**
Dennis Pielken

12:30 Discussion

12:45 Lunch

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

Chair: Steven David Brown

14:00 **Websites and social media: the legal challenges of dealing with electronic evidence in criminal proceedings**
- Principles of dealing with electronic evidence
- Common procedures for recognising and handling evidence on digital devices
- International investigations (search and seizure – obtaining evidence from the Internet, admissibility)
- the challenges in finding the evidence on websites and social media

Joachim Meese

14:45 Discussion

15:00 Break

Objective

The main objective of this seminar is to train EU legal practitioners on the fundamentals of electronic evidence enabling them to gain an overview of the complex challenges related to criminal cases with tech/internet components. This event will address online investigations with particular focus on searches on websites and social media platforms.

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 planned 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 (UK and Denmark do not participate in the Justice Programme 2014-2020).

Venue

Judicial complex (Justiční areál)
Na Míčánkách, 28. pluku
1533/29b, Prague 10 (Praha 10)

CPD

ERA's programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). This event corresponds to **8.5 CPD hours**.

Your contact persons

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

Liz Greenwood
Assistant
Tel.: +49(0)651 9 37 37 322
E-Mail: Egreenwood@era.int

Chair: Laviero Buono

15:30 **Social media and electronic evidence**
How social media networks yield digital evidence of the planning and commission of crimes, and assisted in cyber investigations resulting in the creation of solid cases against the defendants or their acquittals. Presentation of various cases involving Facebook, Twitter, Whatsapp et al.
Patricia Ayodeji

16:30 Discussion

16:45 End of the first day

19:00 Dinner

Tuesday, 19 October 2021

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

Chair: Patricia Ayodeji

09:30 **Computer forensics and electronic evidence in court: issues of authenticity, reliability and credibility with particular reference to data extracted from social media platforms**
John Van Krieken

10.00 Discussion

10:15 **Online investigations and the challenges for the defence**
Muthupandi Ganesan

10:45 Discussion

11:00 Break

Chair: Laviero Buono

11:30 **Handling electronic evidence in courts**
- The importance of the chain of custody in handling evidence
- Trial considerations: methods of presentation and admissibility tests

Claudia Pina

12:00 **E-evidence gathering in the Czech Republic: theory and practice**
Pavel Zeman

12:30 Discussion

12:45 End of seminar and light lunch

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

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.

Seminar

Obtaining e-evidence when investigating and prosecuting crimes

18-19 October 2021 / Event number: 321DT34f/eg

Europäische Rechtsakademie
Academy of European Law
Académie de Droit Européen
Accademia di Diritto Europeo

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.
3. Applications should be submitted before **30 September 2021**.
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 (if your place of work is more than 100km from the venue) 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 can be reimbursed by ERA, only upon receipt of the original hotel invoice, up to €155.00 per night including breakfast, if your place of work is more than 100km from the venue.

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. A certificate of attendance will be distributed at the end of the conference.

Apply for "Obtaining e-evidence when investigating and prosecuting crimes": www.era.int/?130868&en

Language

English

Venue

Judicial complex (Justiční areál)
Na Míčánkách, 28. pluku
1533/29b, Prague 10 (Praha 10)

Contact Person

Liz Greenwood
Assistant
Egreenwood@era.int
+49 651 9 37 37 - 322

Must prove:

Which device used in the offence.

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

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

Identifiers have been redacted

InZeit
Excellence in Acuity

What is the Internet ?

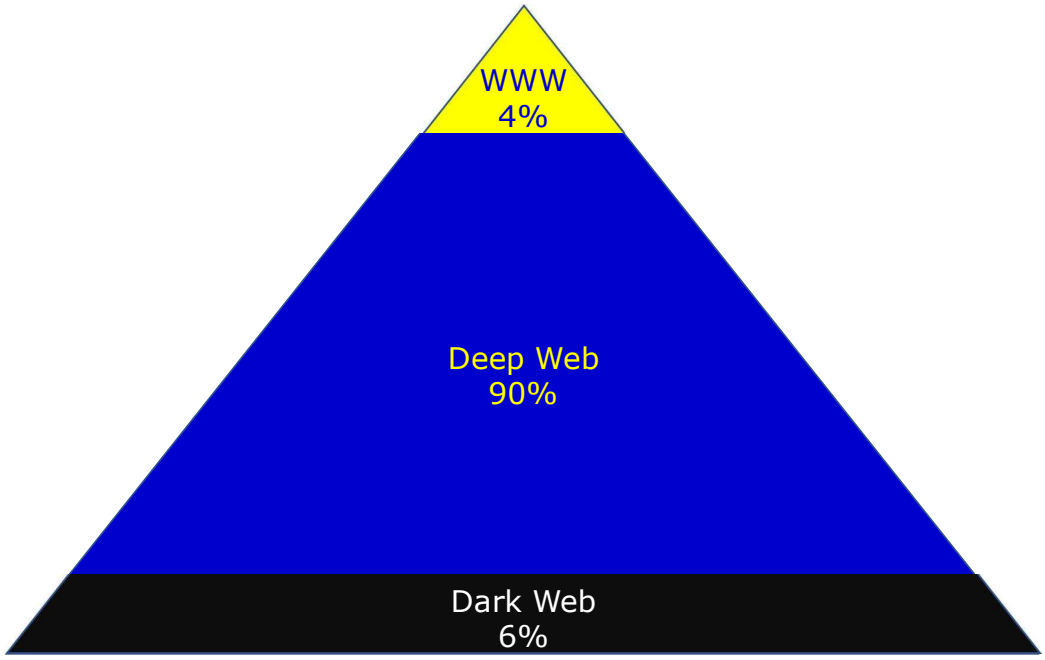
Internet, a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect. Sometimes referred to as a "network of networks"

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

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

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

InZeit
Excellence in Acuity



Indexed by search engines; publicly accessible

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

Special software for access; spies, dissidents & criminals

InZeit
Excellence in Acuity

Data, data everywhere

4.66 billion active internet users worldwide
= 59.5 % global population.
(Jan 2021)

92.6 percent (4.32 billion) access internet **via mobile devices**.

https://www.statista.com/statistics/617136/digital-population-worldwide/

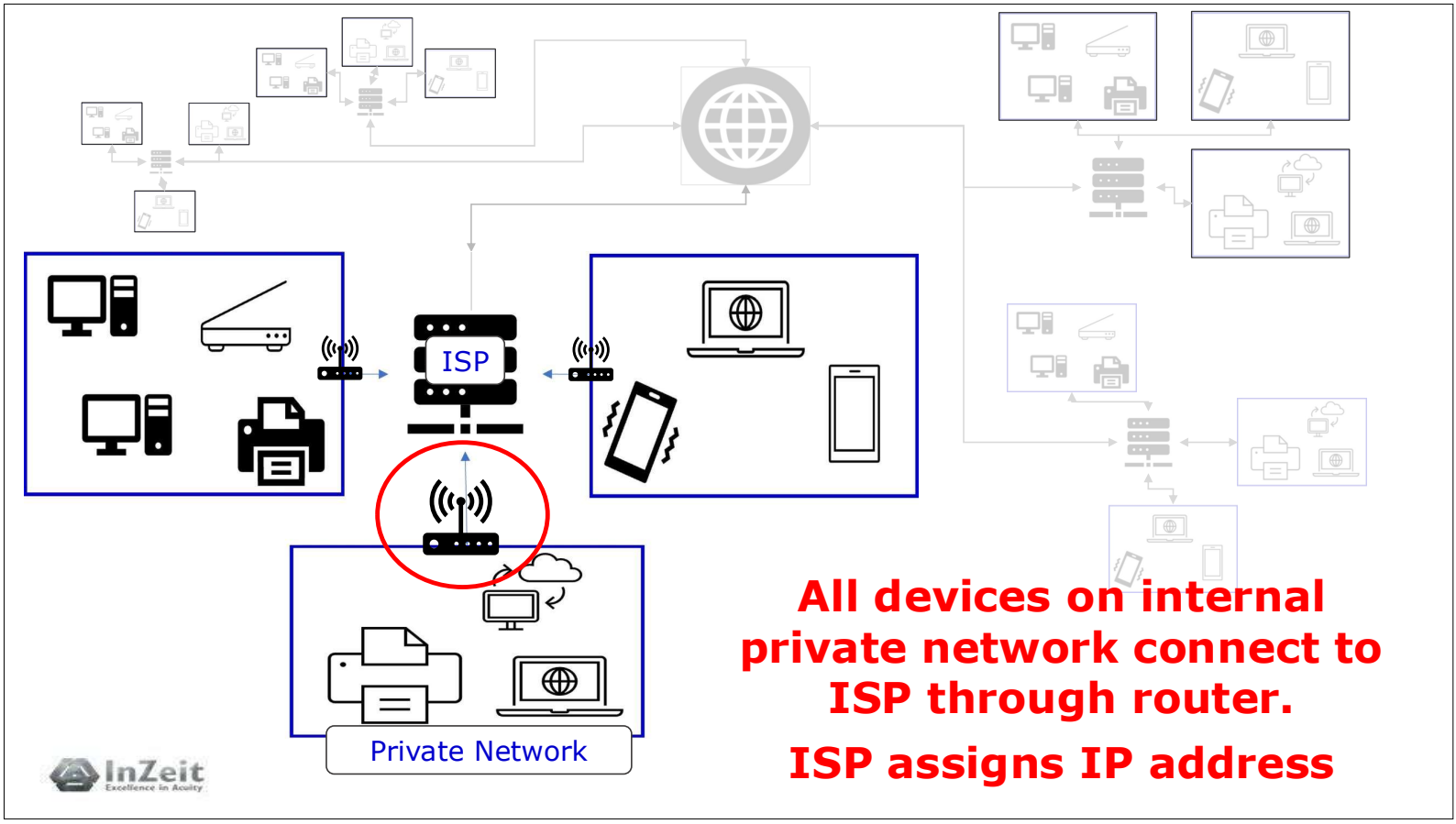
InZeit
Excellence in Acuity

WWW contains **at least 4.13 billion pages**
(July 2021)
https://www.worldwidewebsize.com/

2.5 quintillion bytes of data created daily
(90% world's data created in the last two years).
https://www.the-next-tech.com/blockchain-technology/how-much-data-is-produced-every-day-2019/

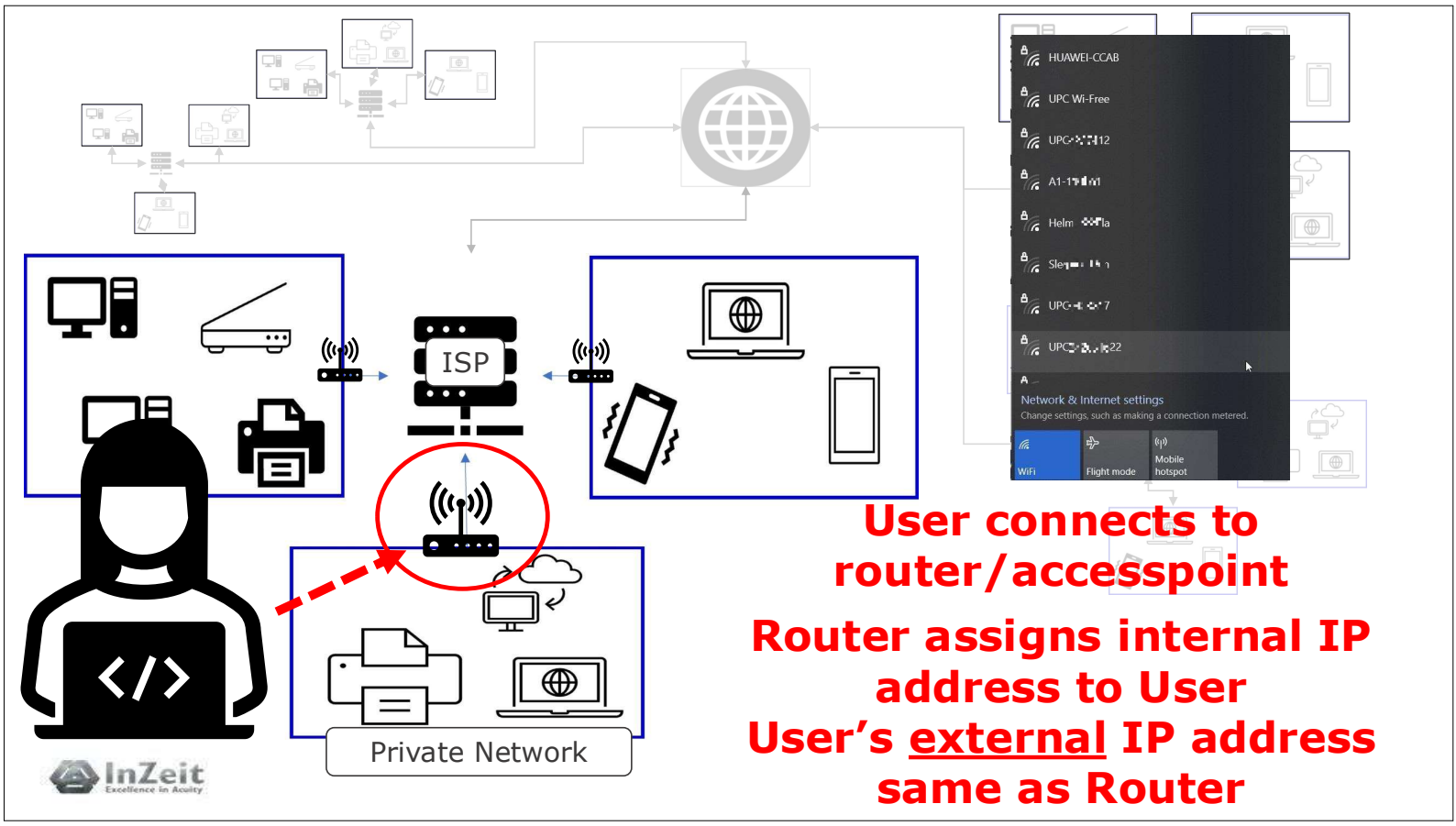
A quintillion =1 followed by 18 zeros
2,500,000,000,000,000,000 bytes per day

InZeit
Excellence in Acuity



All devices on internal private network connect to ISP through router.

ISP assigns IP address



User connects to router/accesspoint

Router assigns internal IP address to User

User's external IP address same as Router

Assigned by Internet Service Provider (ISP)

Addresses Allocated Geographically

(Public) Internet Protocol (IP) Address

Static -v- Dynamic

Your address on the Internet

ISP holds subscriber addresses

InZeit Excellence in Acuity

Two kinds of IP Address:

IPv4 195.243.153.54 = www.era.int

- 4,294,967,296 possible IPv4 addresses
- 4.66 billion active internet users worldwide (i.e. not enough!)

IPv6

2001:0db8:85a3:0000:0000:8a2e:0370:7334

- 8 sets of 4 hexadecimal digits (hexadecimal = $base_{16}$ numbers)
- 340 undecillion possible IPv6 addresses
- More than enough for everyone

InZeit Excellence in Acuity

"You can find a suspect or victim through the IP Address"

Who thinks 'Yes'?

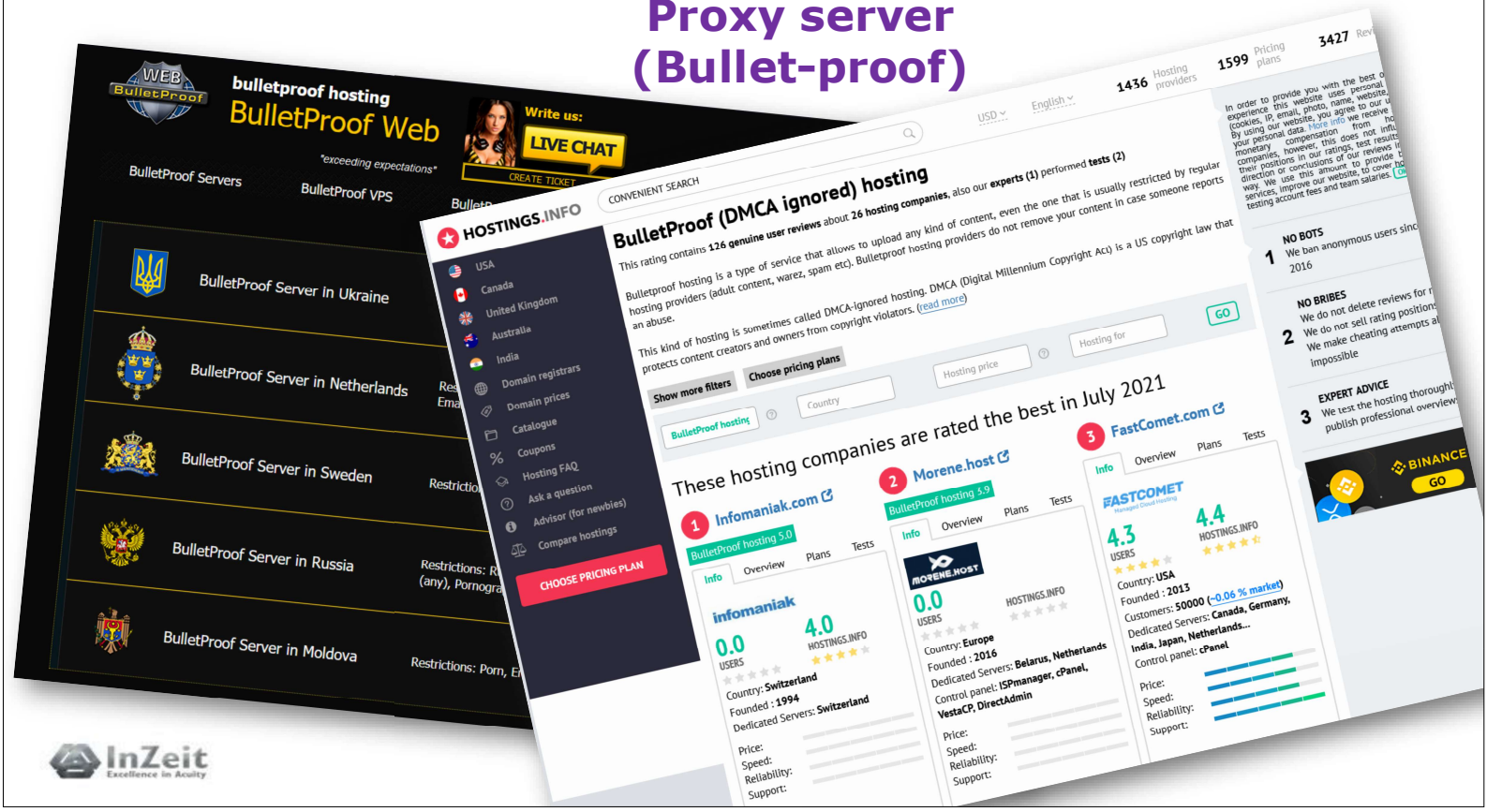
InZeit
Excellence in Acuity

'Yes' … 'but'

- **Use of public wifi Access Point (bar/hotel/airport/library)**
- **Use of unsecure domestic wifi router**
- **Carrier Grade NAT** (Network Address Translation)
- **Proxy Servers**
- **VPNs**
- **Anonymisers like TOR**

InZeit
Excellence in Acuity

Proxy server (Bullet-proof)



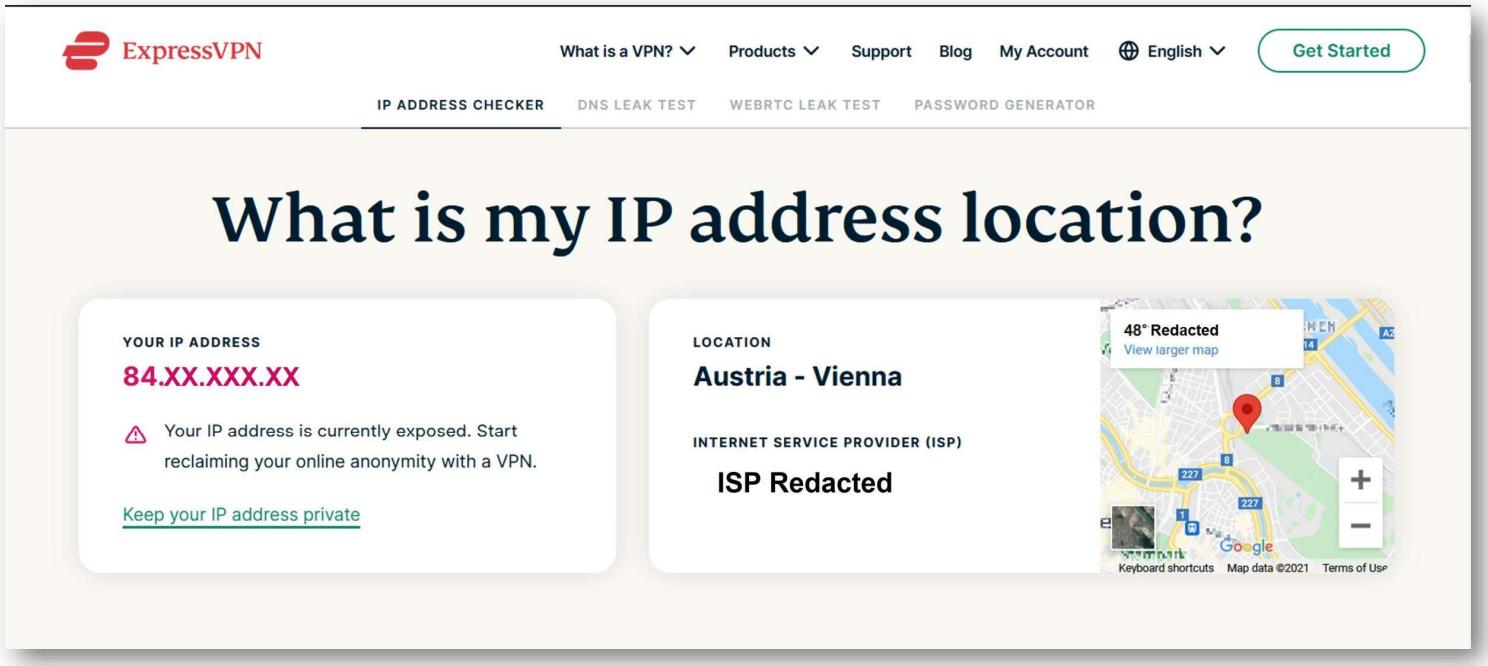
InZeit
Excellence in Acuity

VPN

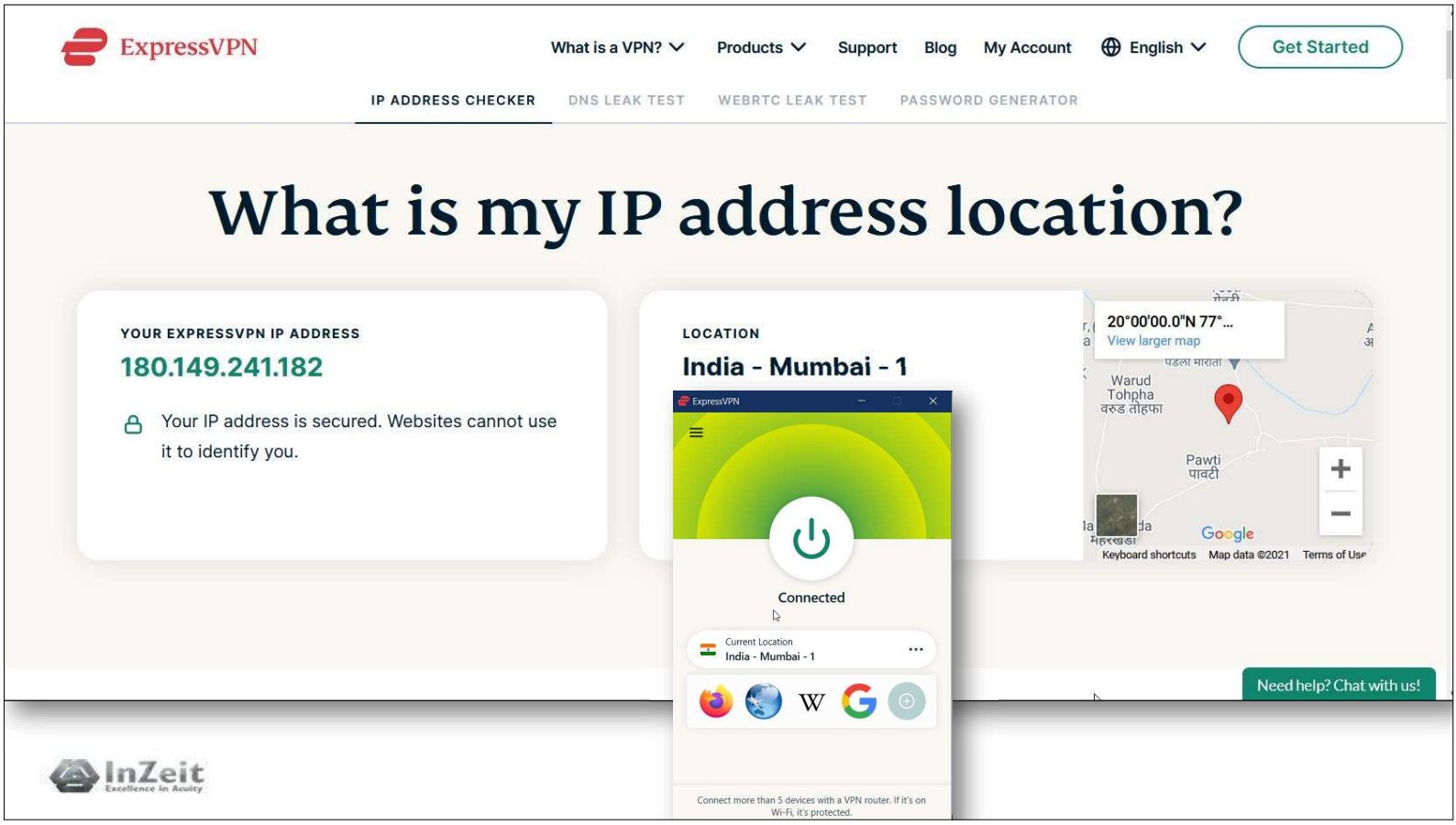
Virtual Private Network

Proxy server with data encryption

InZeit
Excellence in Acuity



(IP Addresses assigned regionally)



No central control

All websites end with .onion

Can be used to access DarkNet

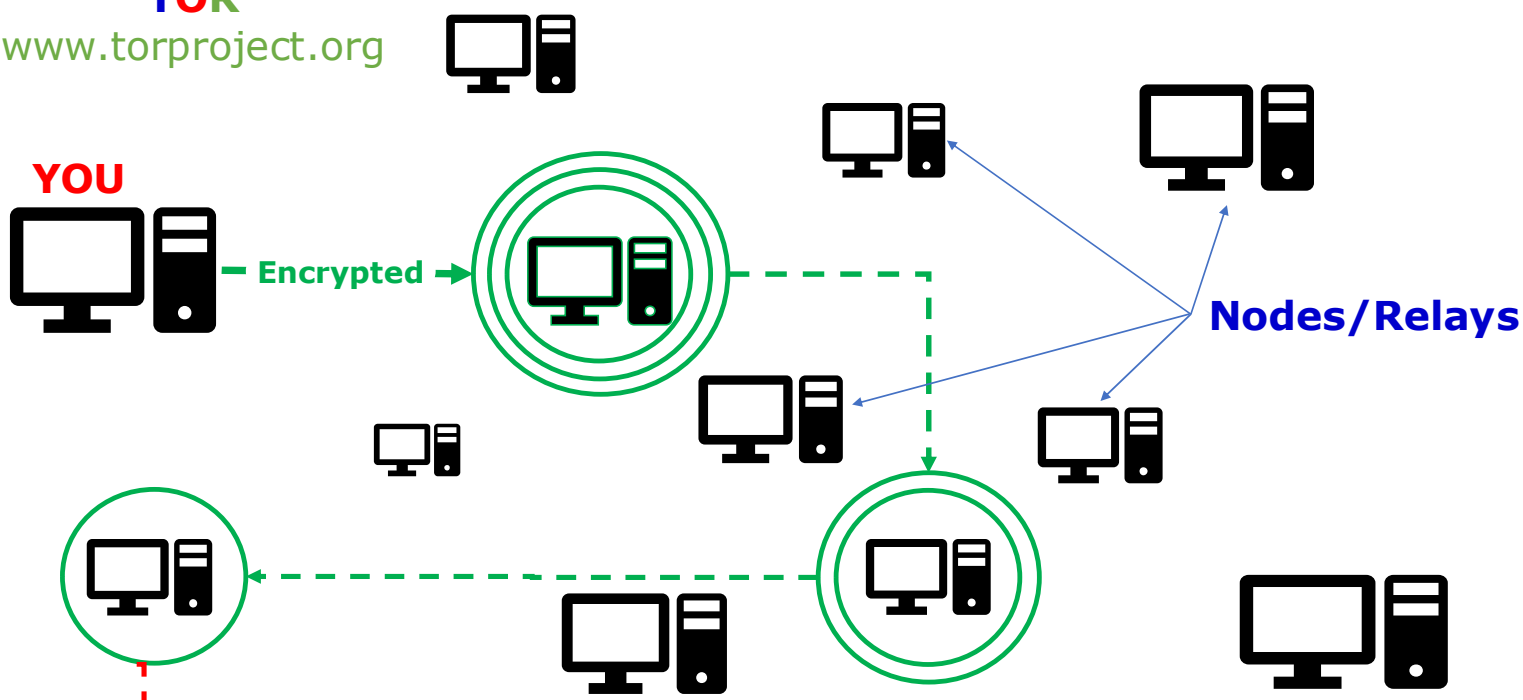
TOR
The Onion Router

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

'Anonymising technology' (there are others)

InZeit Excellence in Acuity

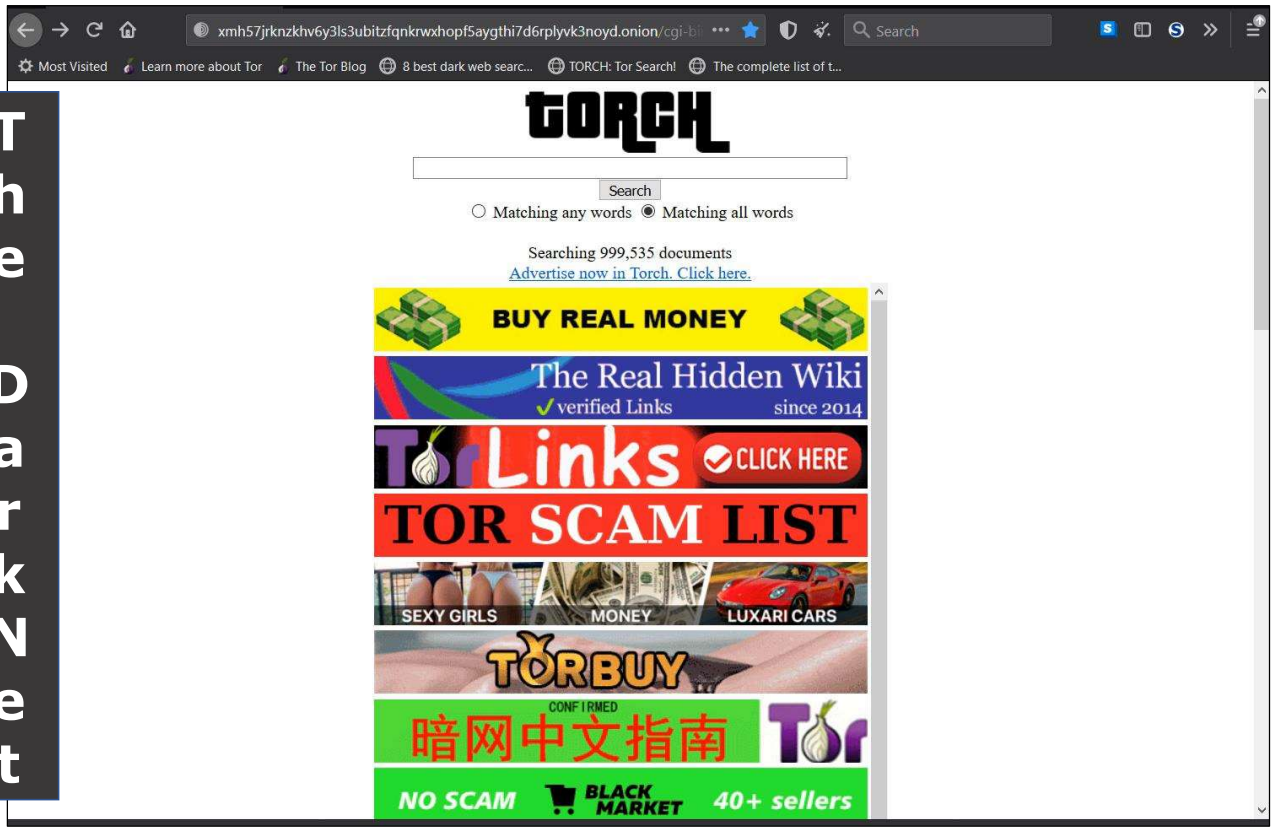
TOR
www.torproject.org



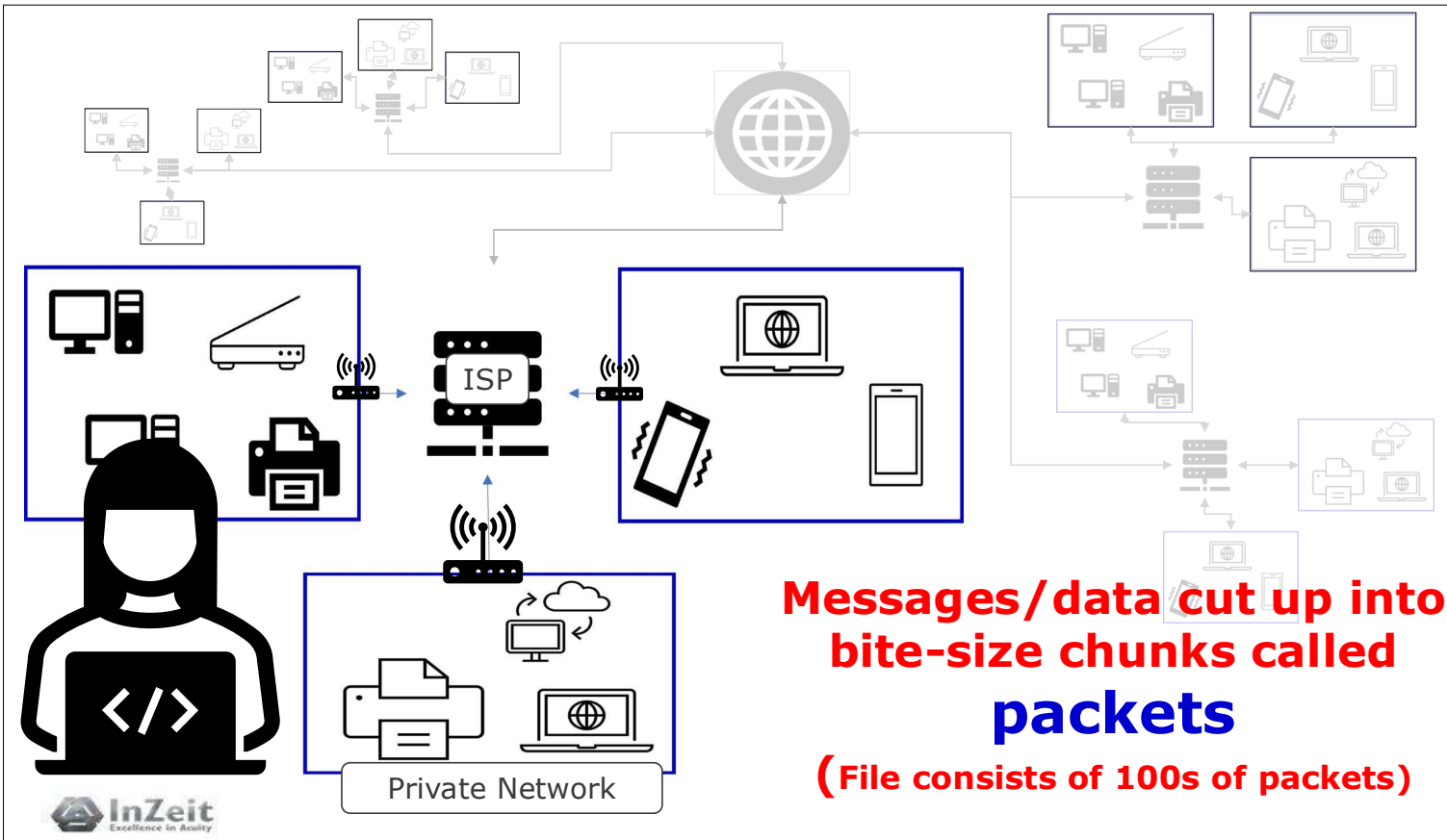
InZeit Excellence in Acuity

TOR

The DarkNet



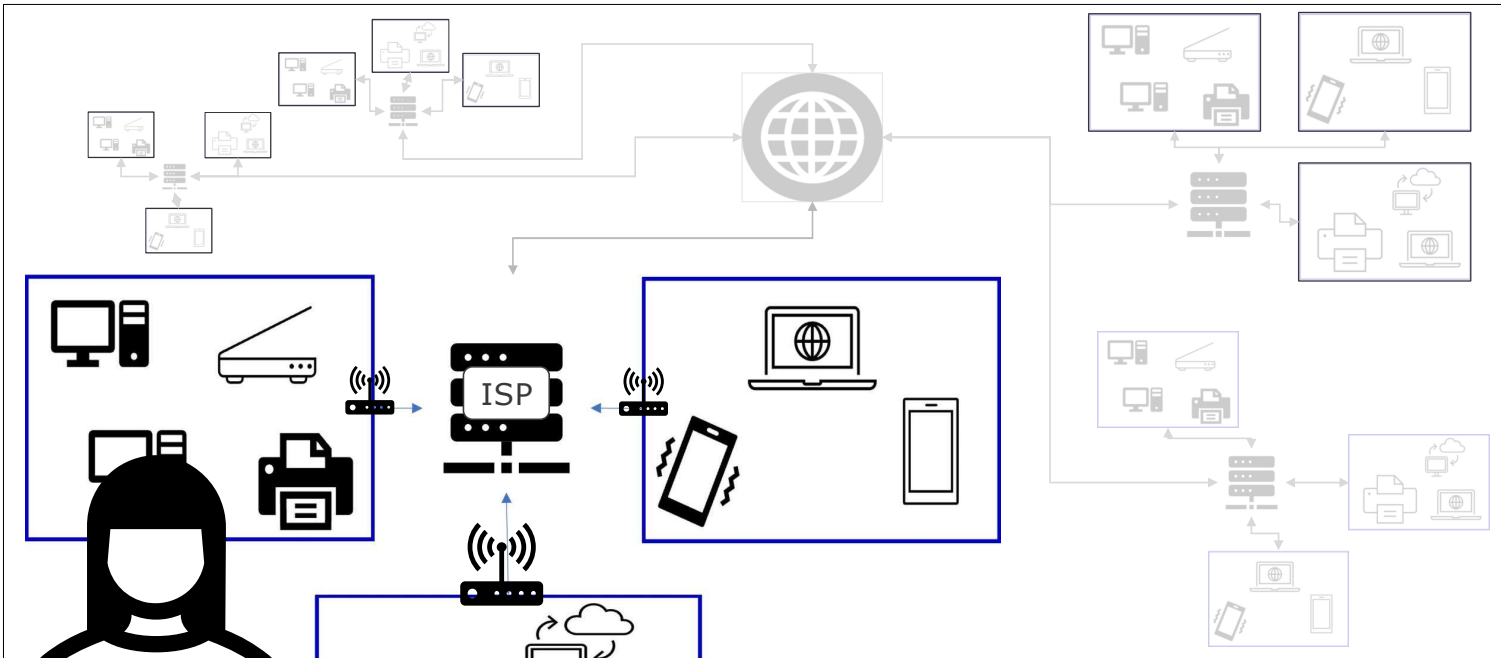
InZeit
Excellence in Acuity



Messages/data cut up into bite-size chunks called packets

(File consists of 100s of packets)

InZeit
Excellence in Acuity



Each packet sent separately (take different route) to destination

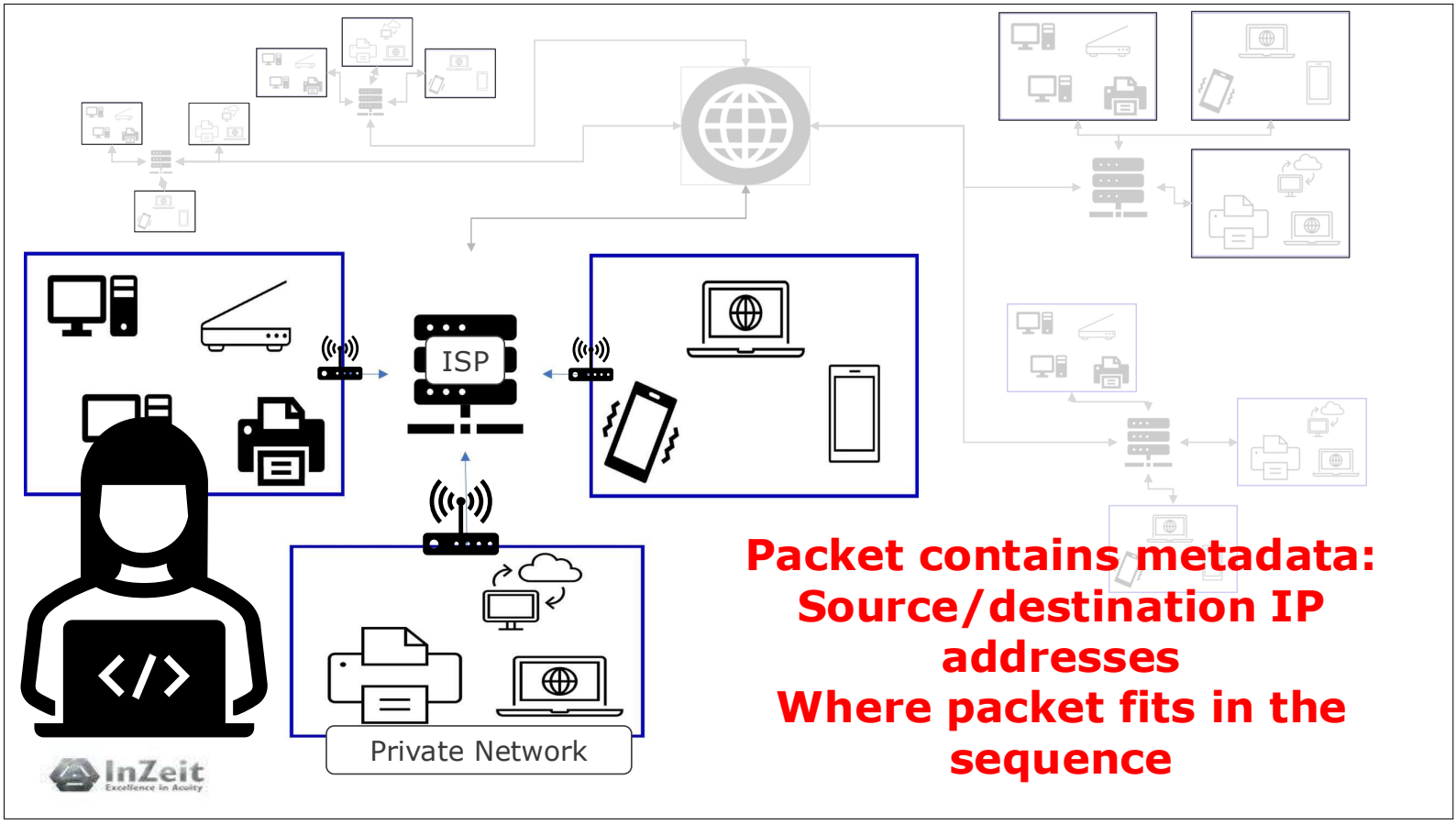
InZeit
Excellence in Acuity

```
Administrator: Command Prompt

Microsoft Windows [Version 10.0.19042.1083]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>tracert era.int

Tracing route to era.int [195.243.153.54]
over a maximum of 30 hops:

  1     3 ms     3 ms     4 ms  compalhub.home [192.168.0.1]
  2    23 ms    23 ms    13 ms  217-[illegible].static.upcbusiness.at [217.[illegible]]
  3    14 ms    15 ms    15 ms  217-[illegible].static.upcbusiness.at [217.[illegible]]
  4    15 ms    14 ms    20 ms  80.157.204.97
  5    35 ms    34 ms    35 ms  p5b17f691.dip0.t-ipconnect.de [91.23.246.145]
  6    35 ms    33 ms    35 ms  87.190.102.6
  7    33 ms    31 ms    32 ms  195.243.153.54

Trace complete.

C:\WINDOWS\system32>
```

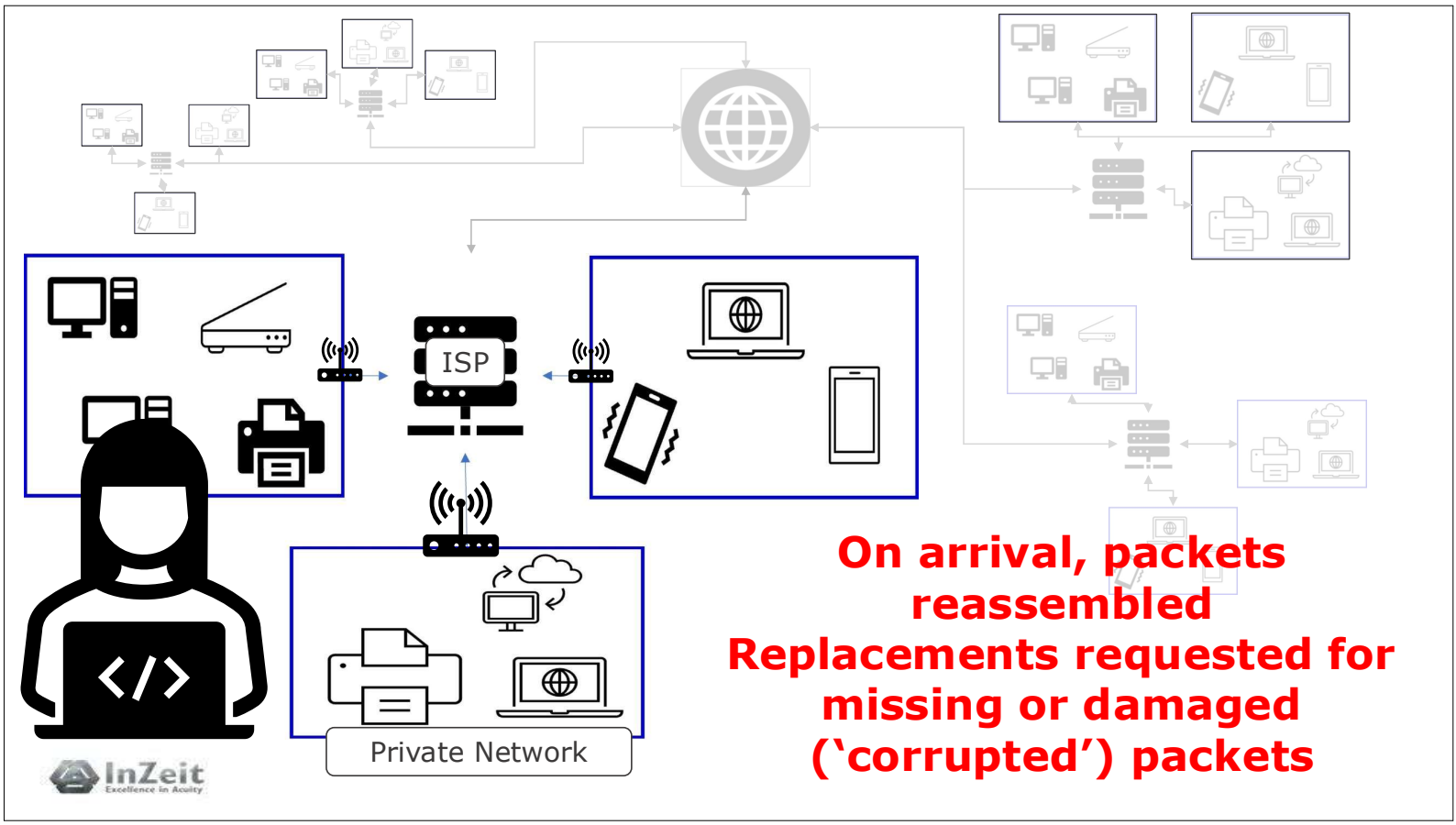
7 Hops

InZeit
Excellence in Acuity

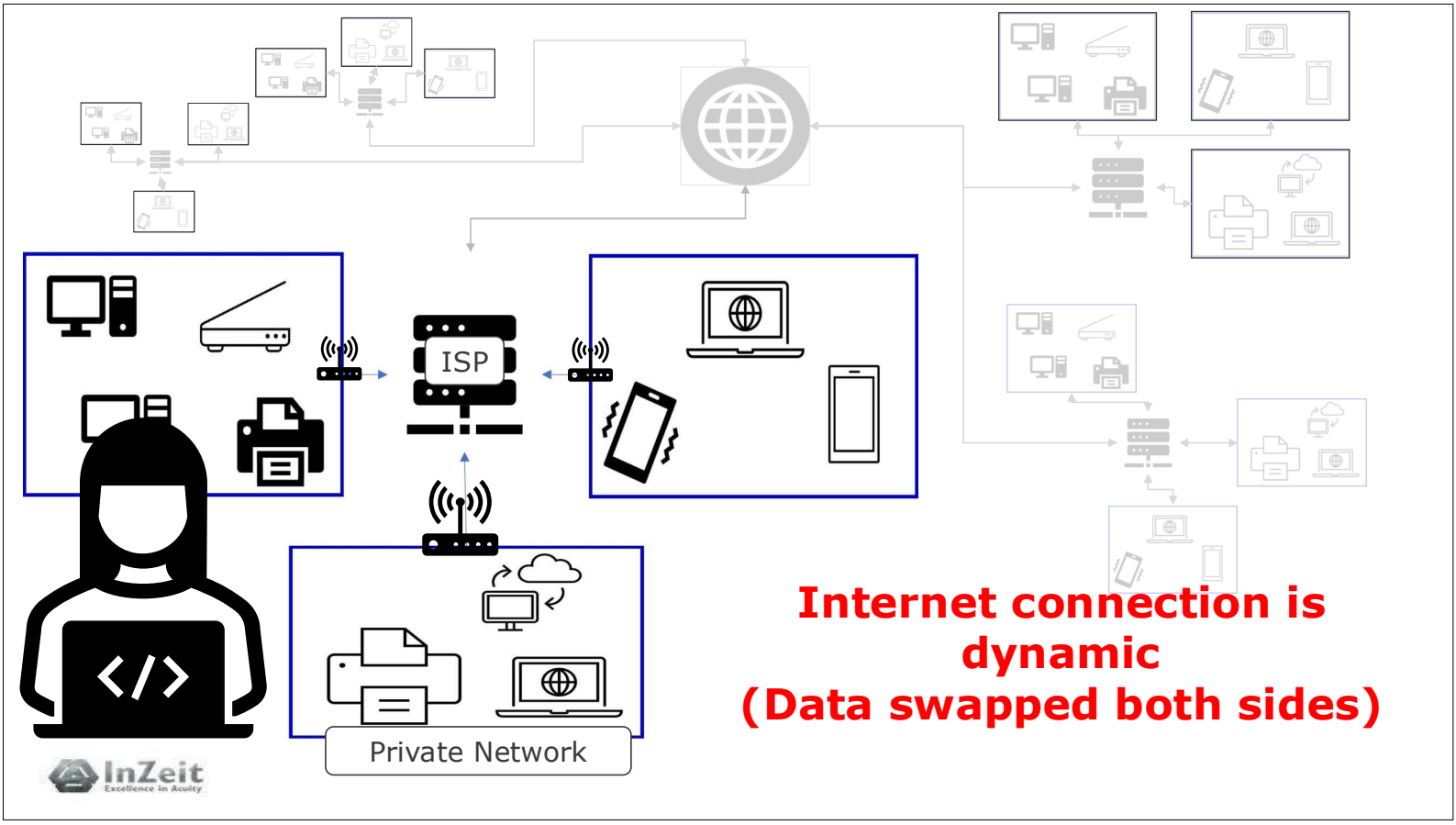
C:\WINDOWS\system32> tracert [website address]



Packet contains metadata:
Source/destination IP addresses
Where packet fits in the sequence

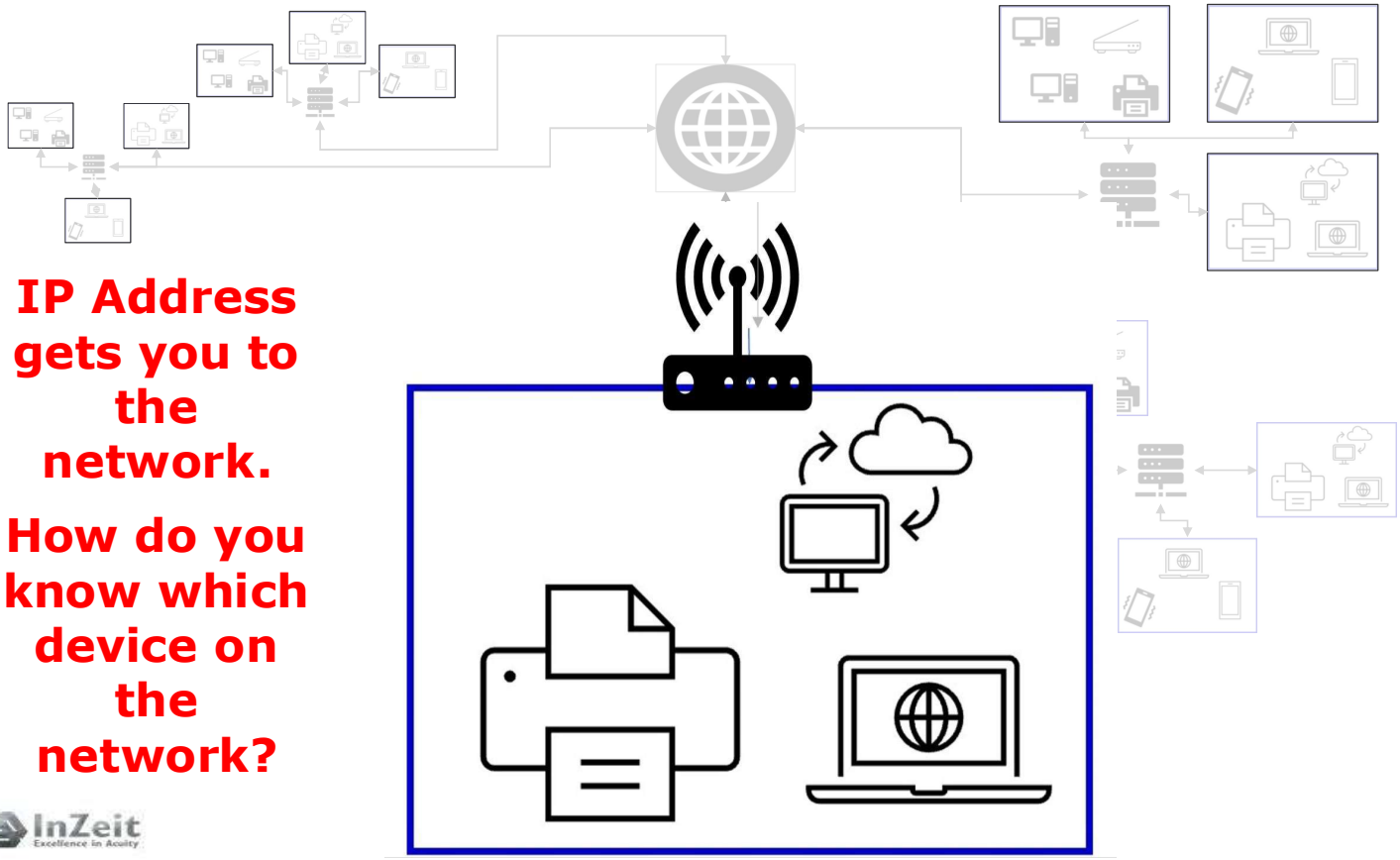


On arrival, packets reassembled
Replacements requested for missing or damaged ('corrupted') packets



Try it yourself:

clickclickclick.click



IP Address gets you to the network.

How do you know which device on the network?

InZeit Excellence in Acuity

Identifying a Device on Network

MAC (Media Access Control) address

- Identifies a device on a private network
- Burnt into Network Interface Card (hardware that connects to Internet)

On mobile device (phone):

IMEI number
(International Mobile Equipment Identity)

- IMEI hardcoded into phone by manufacturer
- Dial *#06#
- Can be used to blacklist

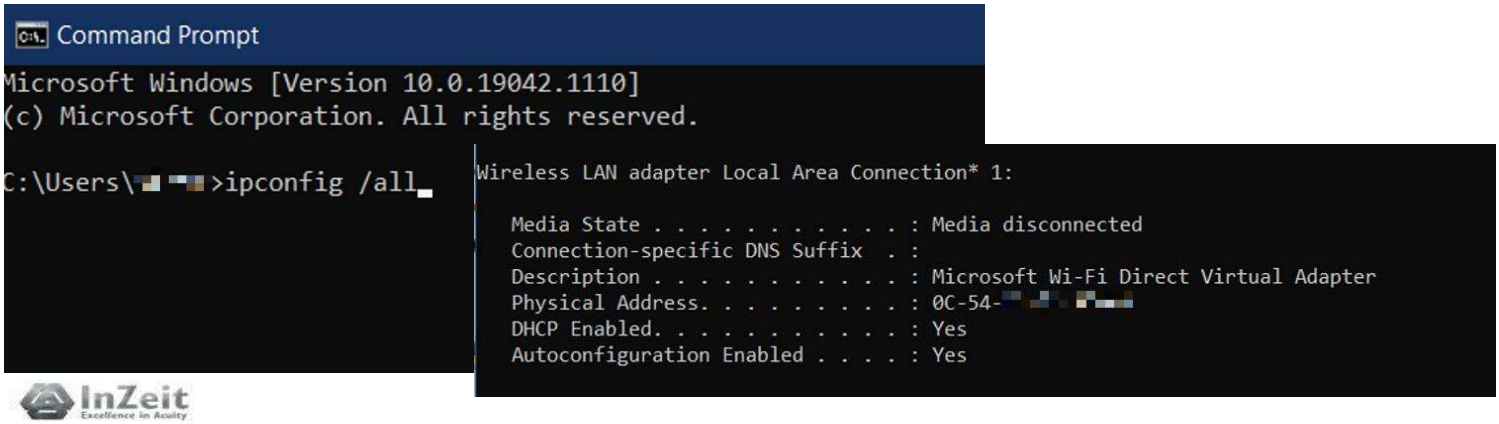
IMSI number
(International Mobile Subscriber Identity)

- IMSI number hardcoded into SIM card
- Identifies SIM to phone porvider

InZeit Excellence in Acuity

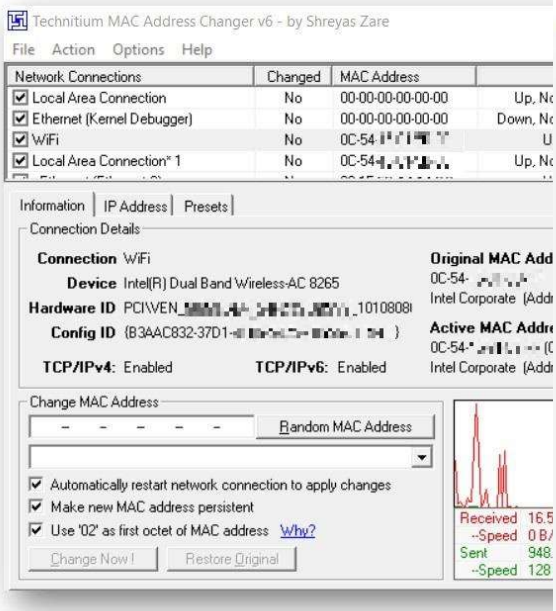
How to find your MAC Address (in Windows)

1. RClick on windows icon bottom left of screen
2. Open search & type **cmd.exe** into search window
3. Click on open cmd.exe.
4. A black window will open with the title 'Command Prompt'
5. Type: **ipconfig /all**
6. Look for the physical address



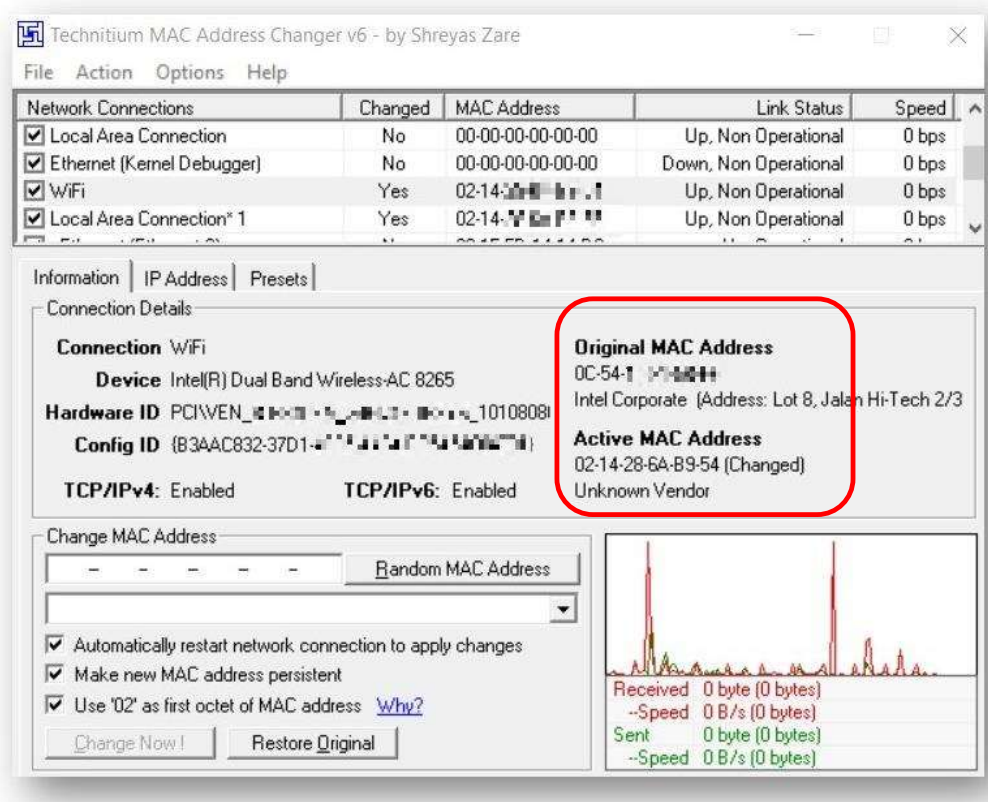
InZeit Excellence in Acuity

Spoofing MAC Address



Technitium MAC Address Changer

A freeware utility to spoof MAC address instantly



InZeit Excellence in Acuity

Moral of the story:

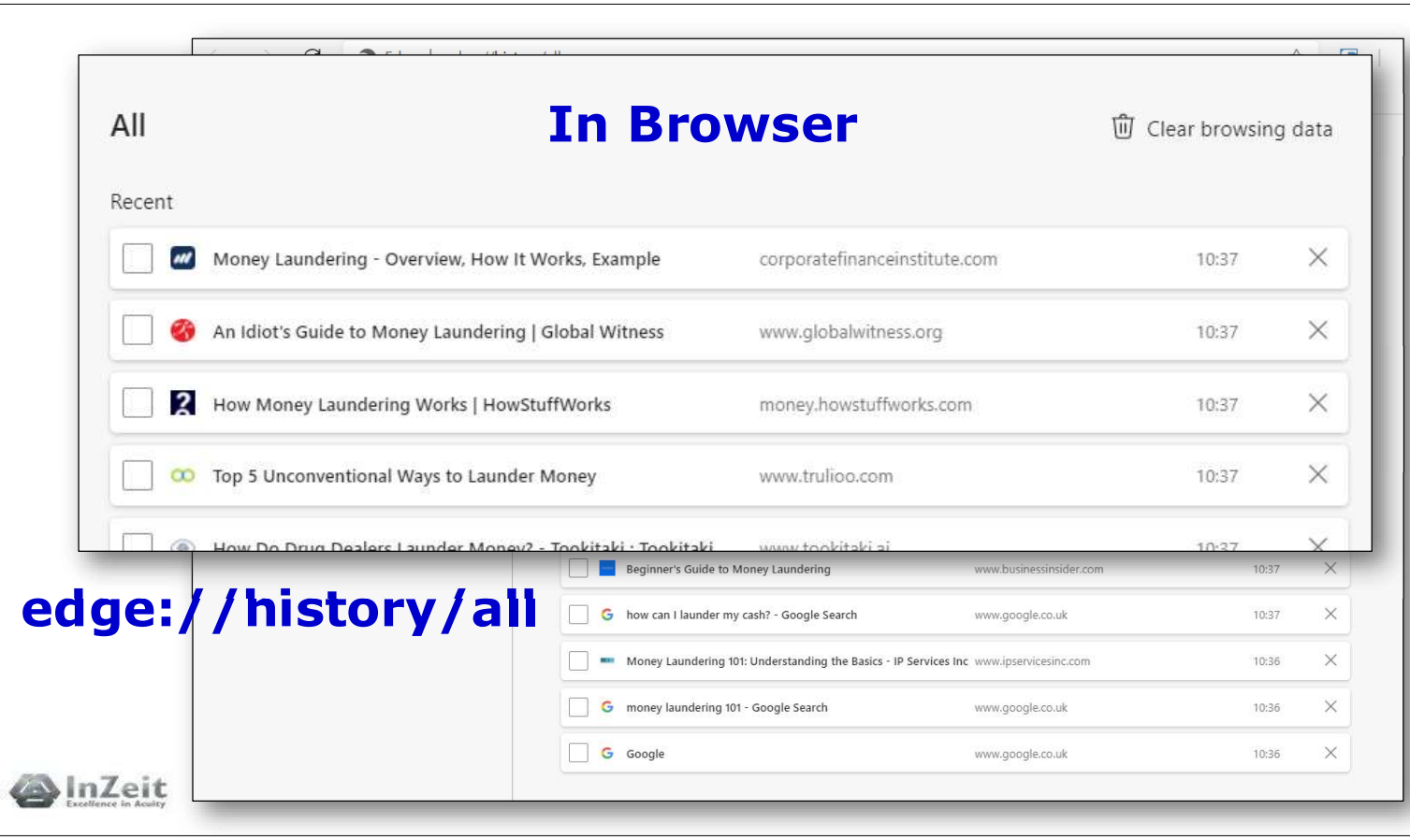
Can’t take anything for granted

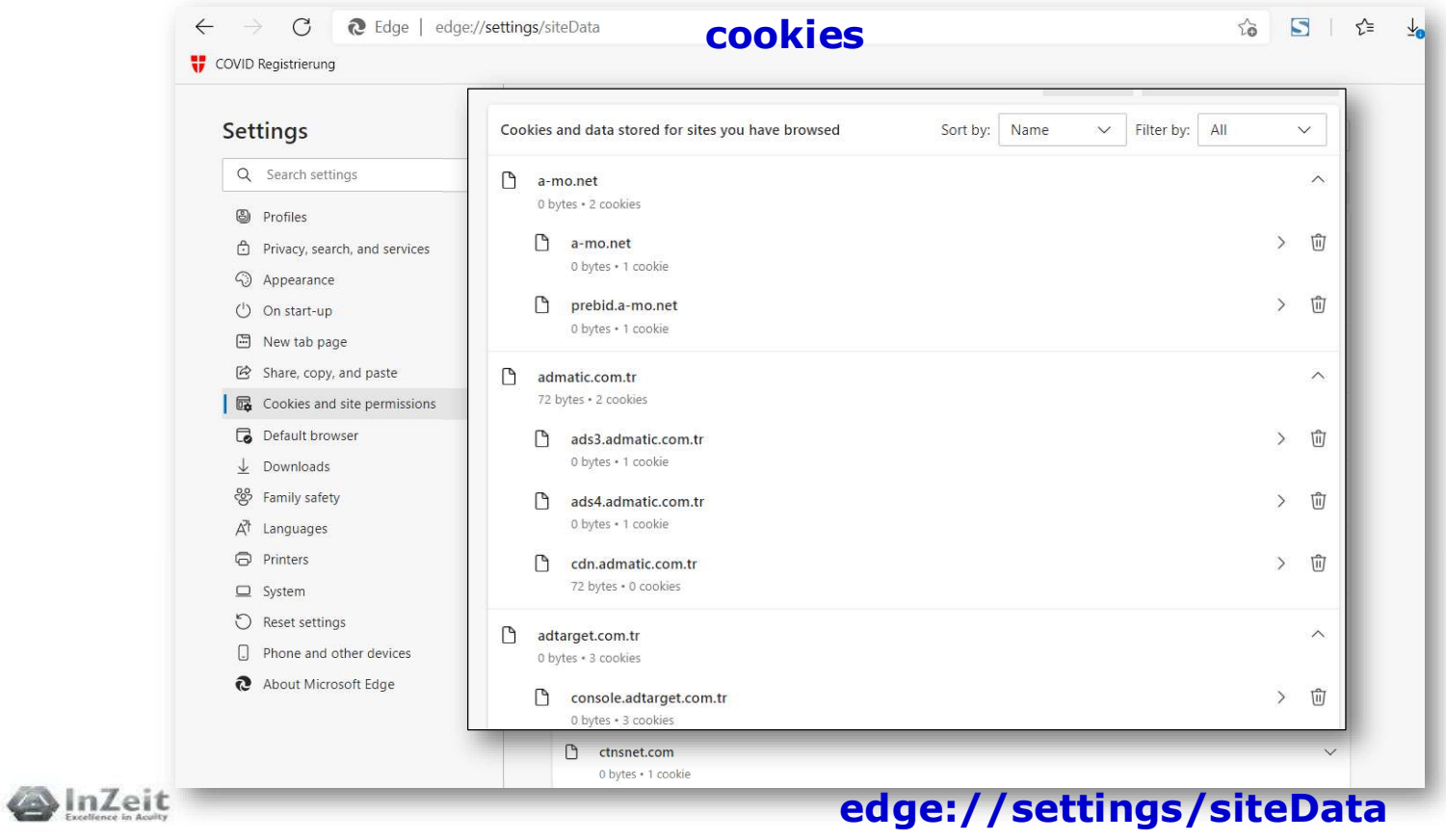
(fortunately most crooks not so sophisticated)

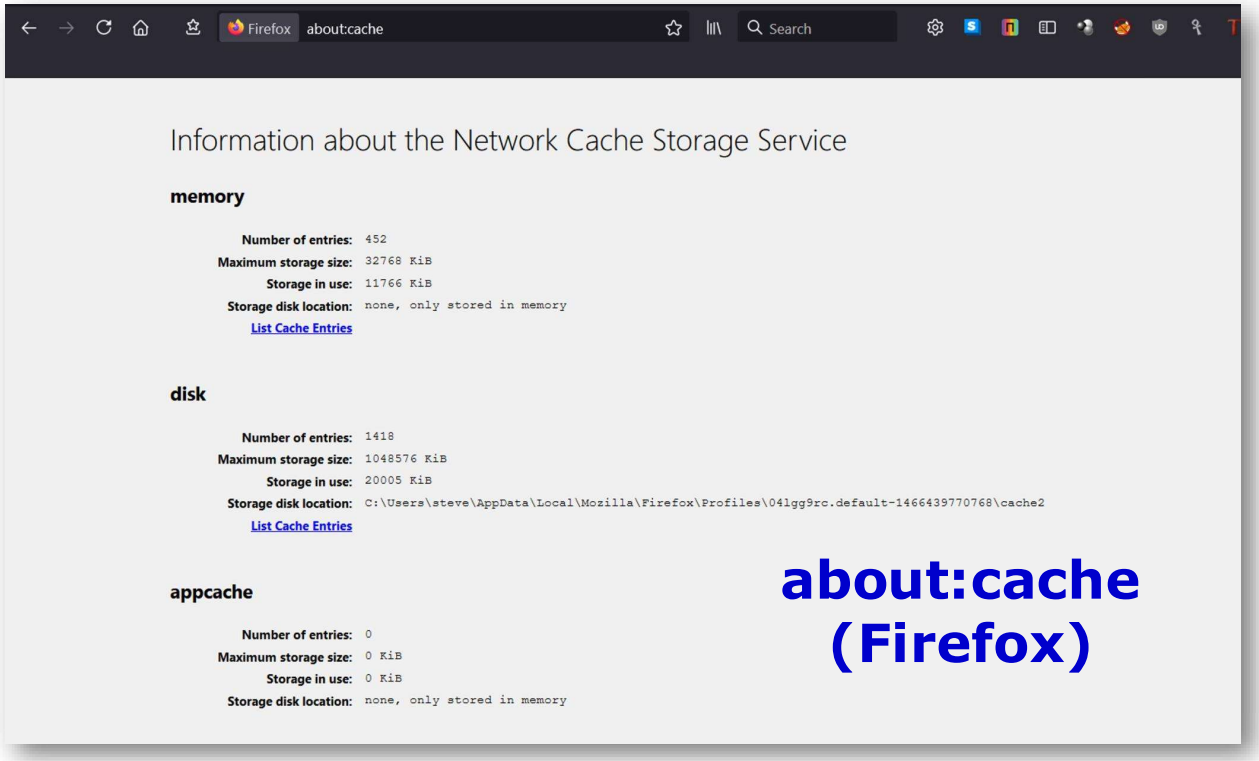
InZeit
Excellence in Acuity

All you need is logs

InZeit
Excellence in Acuity


All
In Browser
Clear browsing data
Recent
Money Laundering - Overview, How It Works, Example
corporatefinanceinstitute.com
10:37
An Idiot's Guide to Money Laundering | Global Witness
www.globalwitness.org
10:37
How Money Laundering Works | HowStuffWorks
money.howstuffworks.com
10:37
Top 5 Unconventional Ways to Launder Money
www.trulioo.com
10:37
Beginner's Guide to Money Laundering
www.businessinsider.com
10:37
how can I launder my cash? - Google Search
www.google.co.uk
10:37
Money Laundering 101: Understanding the Basics - IP Services Inc
www.ipservicesinc.com
10:36
money laundering 101 - Google Search
www.google.co.uk
10:36
Google
www.google.co.uk
10:36
edge://history/all

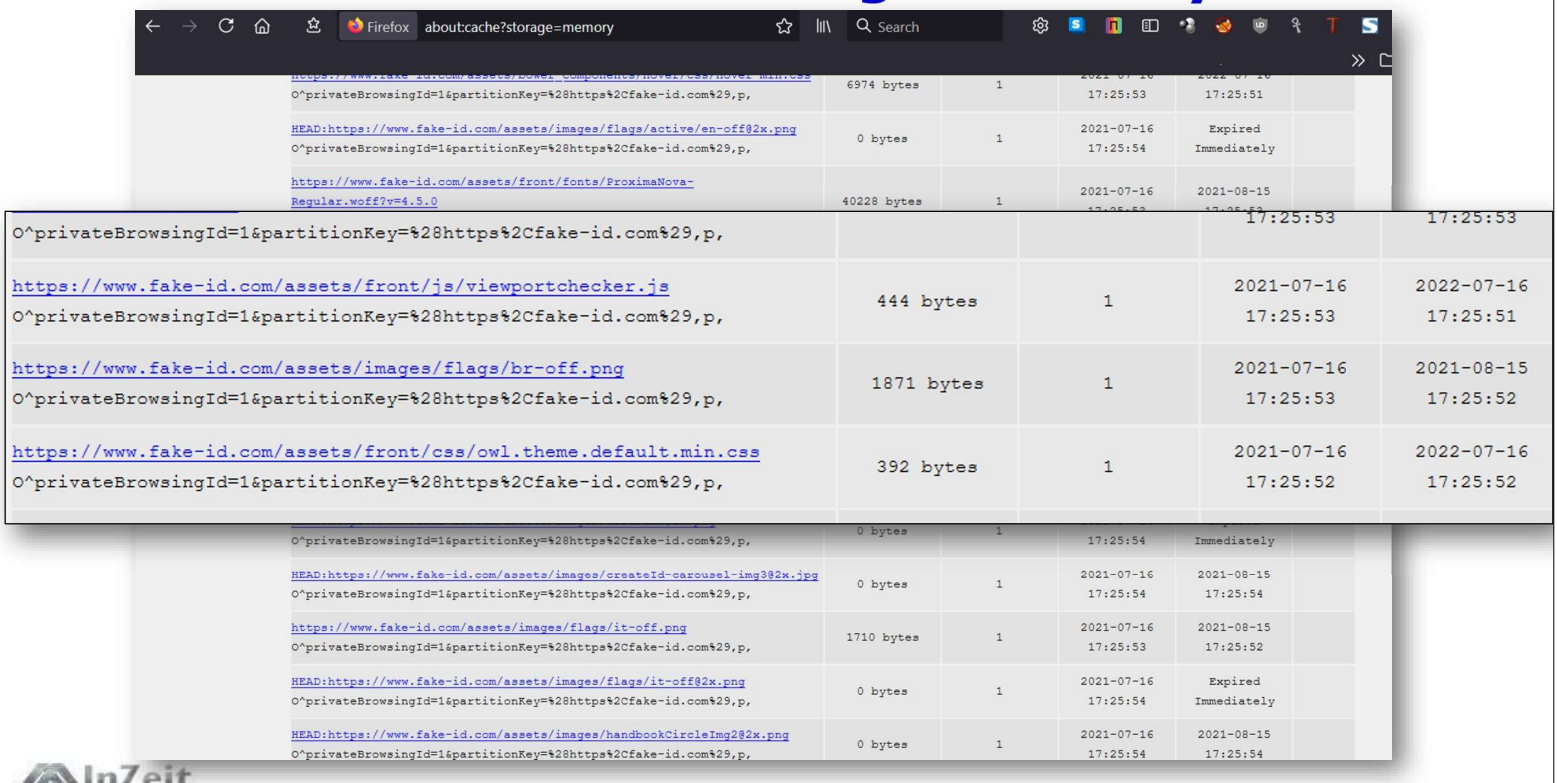

cookies
Edge | edge://settings/siteData
COVID Registrierung
Settings
Search settings
Profiles
Privacy, search, and services
Appearance
On start-up
New tab page
Share, copy, and paste
Cookies and site permissions
Default browser
Downloads
Family safety
Languages
Printers
System
Reset settings
Phone and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



about:cache (Firefox)

InZeit Excellence in Acuity

about:cache?storage=memory



InZeit Excellence in Acuity

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

Username weirdo0000

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

Encrypted chats discussed with seller:

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

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

InZeit Excellence in Acuity

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

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

Google searches:

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

On LG Nexus smartphone searched Yahoo for:

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

InZeit Excellence in Acuity

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

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

Try this out:

https://webkay.robinlinus.com/

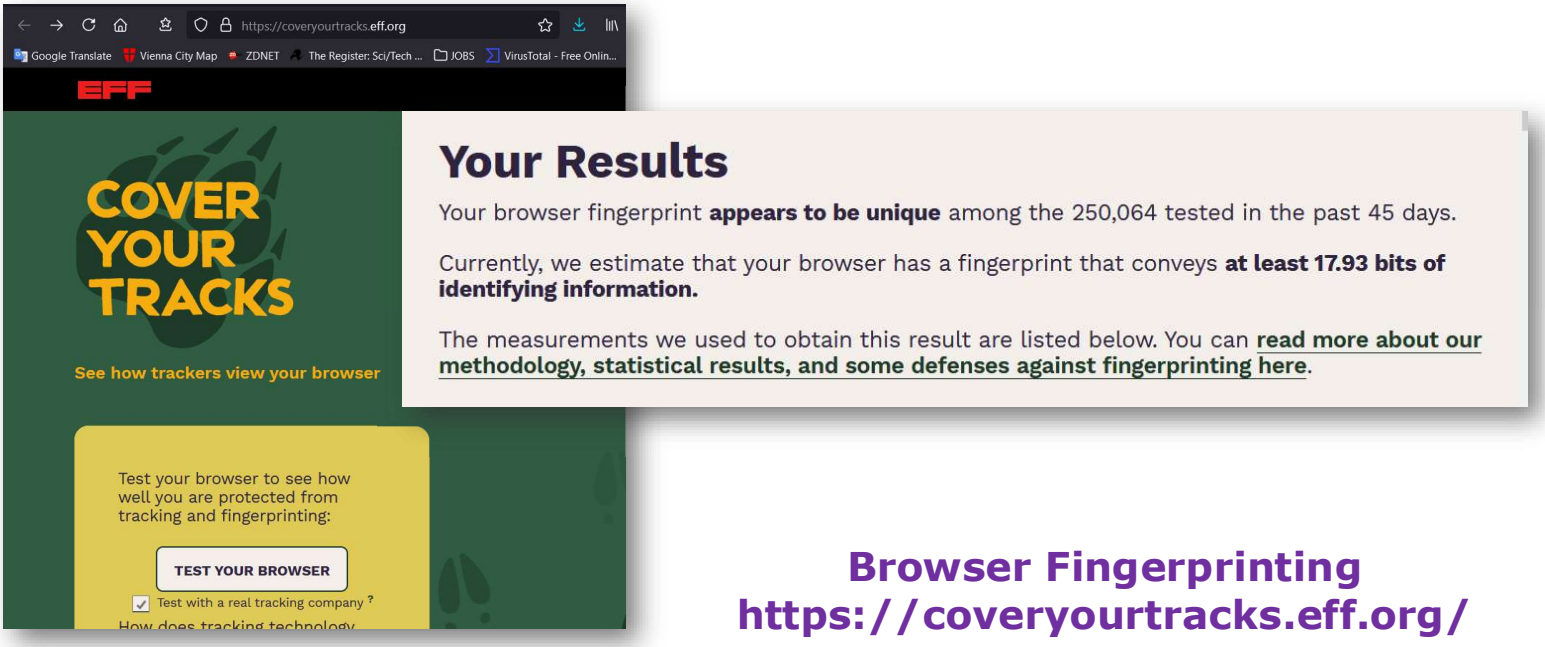
InZeit
Excellence in Acuity

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

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

InZeit
Excellence in Acuity

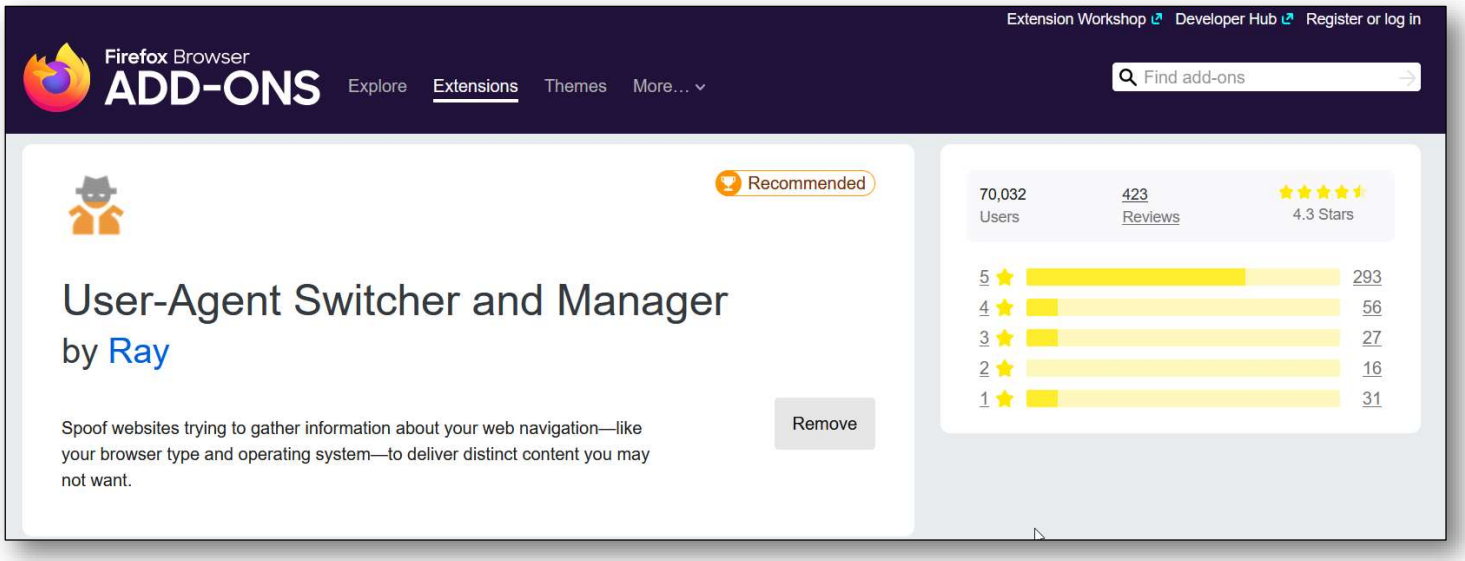
https://us.norton.com/internetsecurity-privacy-how-data-brokers-find-and-sell-your-personal-info.html



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

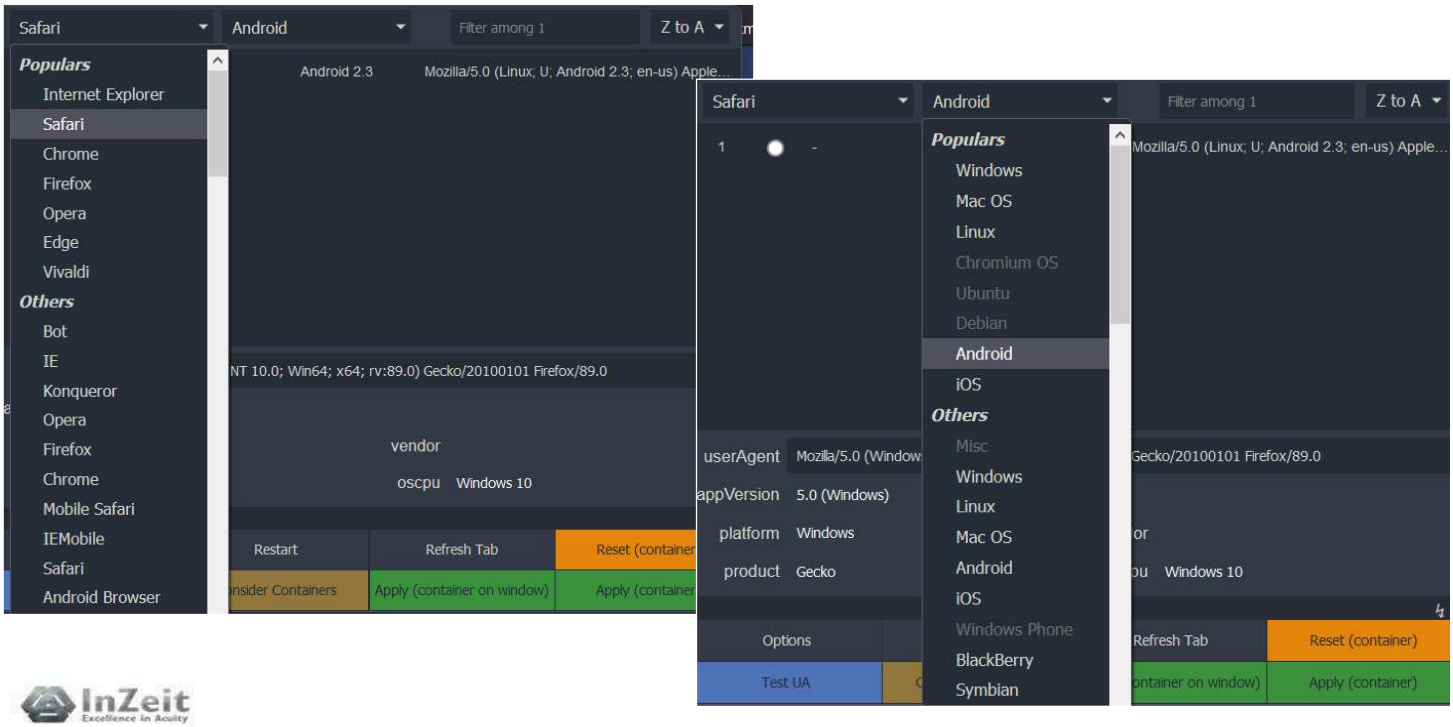
InZeit
Excellence in Acuity

Browser fingerprint can also be faked:

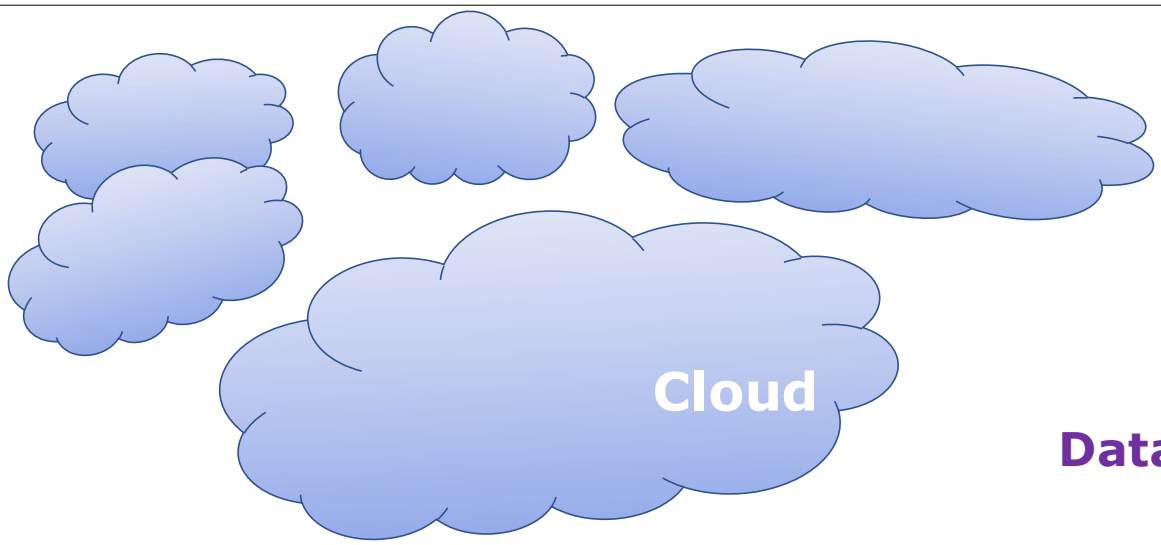


InZeit
Excellence in Acuity

Browser fingerprint can also be faked:



InZeit
Excellence in Acuity

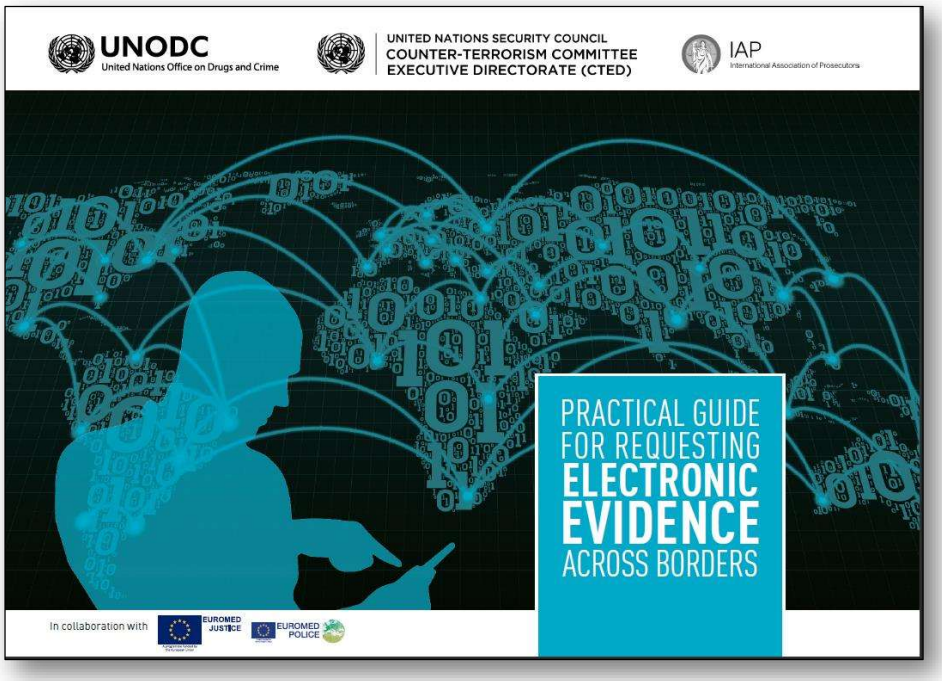


Data is elsewhere

In more than one country, moved from one to another

Cloud service may not know where it is at a given time

InZeit
Excellence in Acuity



https://sherloc.unodc.org/cld/en/publications/practical-guide/practical-guide.html

InZeit Excellence in Acuity

Free download for staff of criminal justice authorities

Internet of Things

Estimated 22 billion -50 billion devices

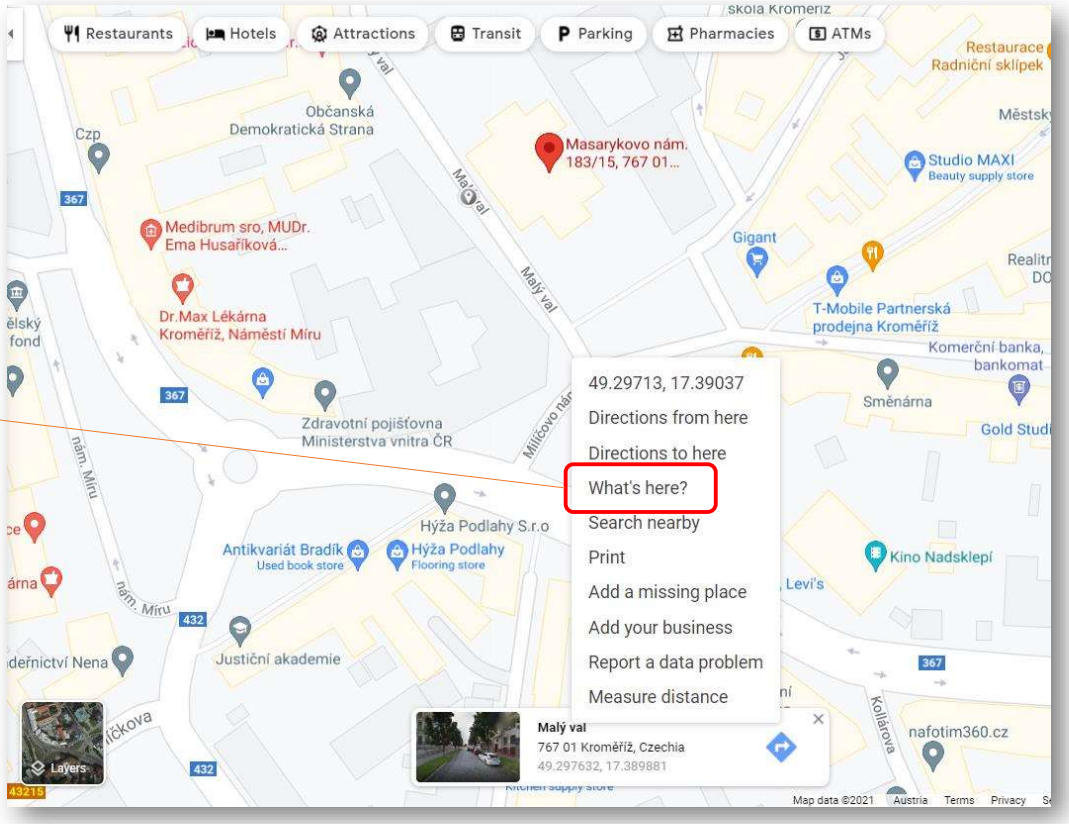
All connected

All generating & logging data

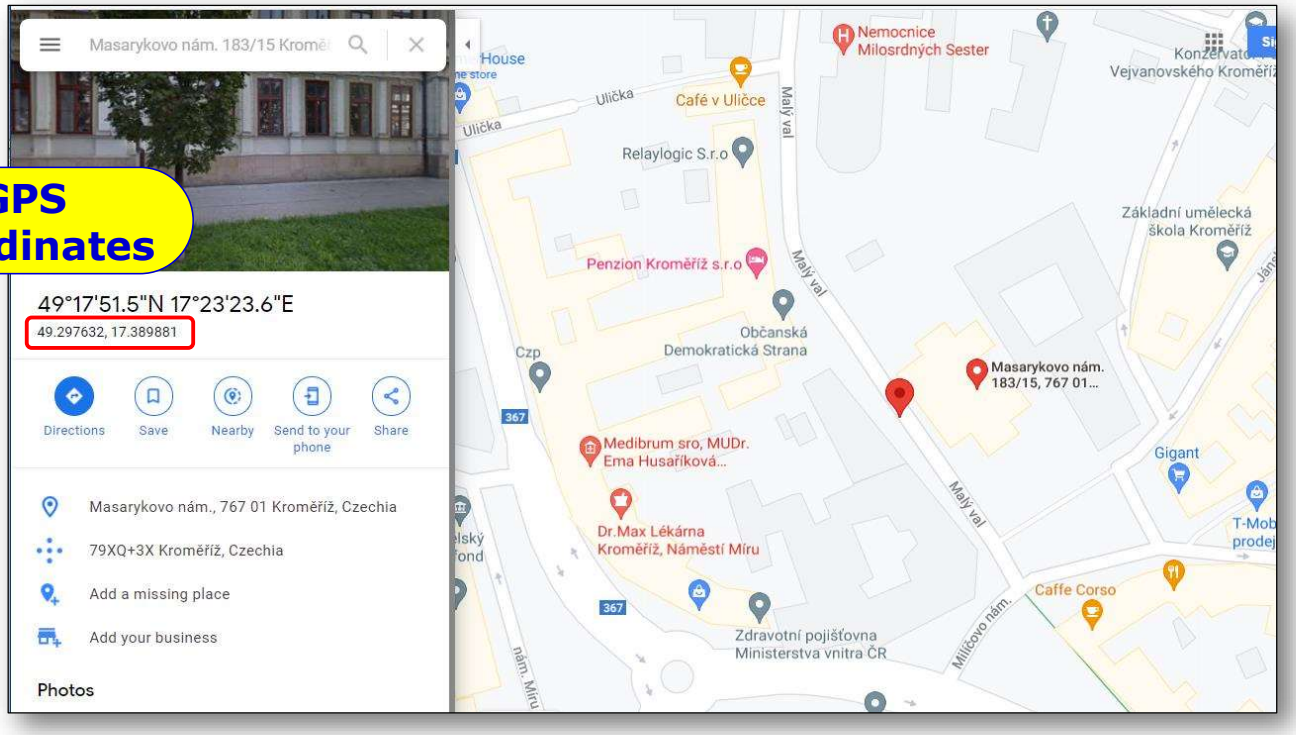
InZeit Excellence in Acuity

Masarykovo nám. 183/15
Kroměříž
767 01

RClick

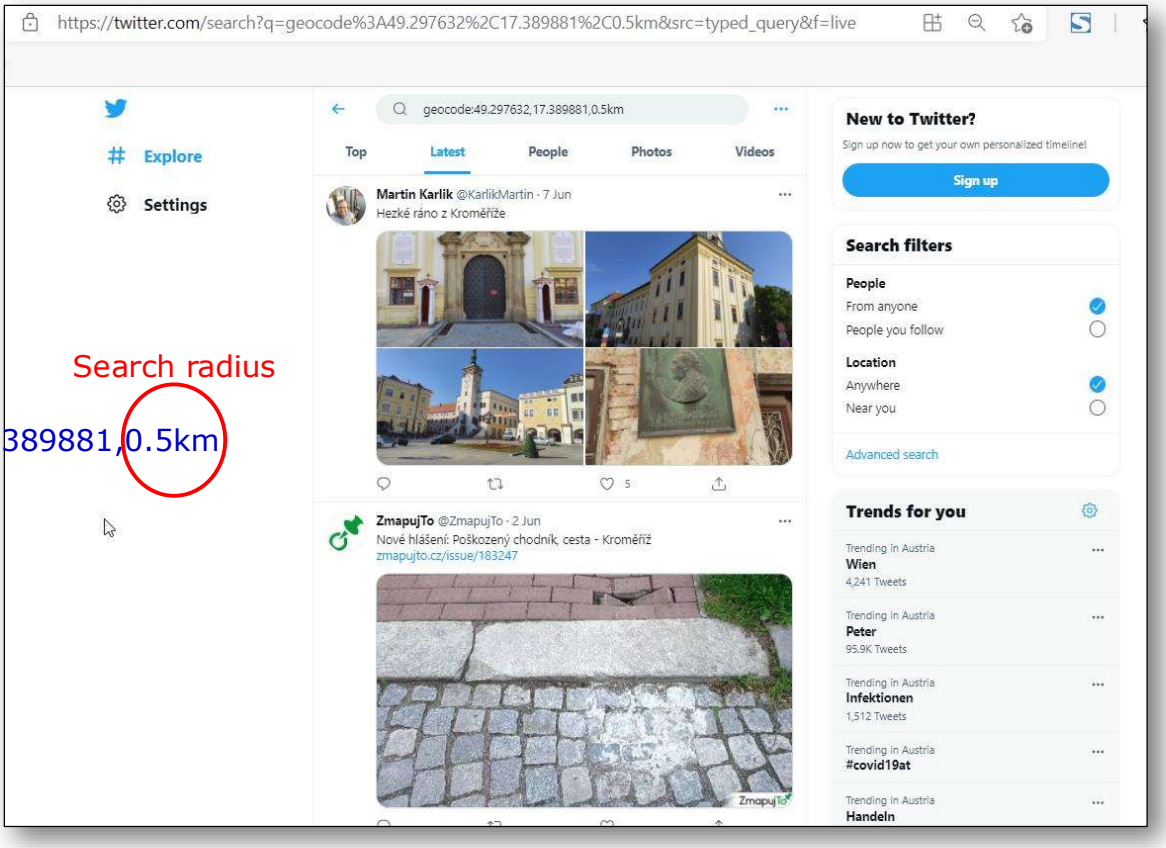


GPS Coordinates



Search radius

geocode:49.297632,17.389881,0.5km



InZeit
Excellence in Acuity

Geofence Warrants & Google's Sensorvault

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

Milwaukee USA June 2017

Middle of the night
Woman car jacked by 2 males

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

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

(Shortly before the carjacking another woman reported to police being harassed by two men (one with baseball bat))

Geofence Warrant sought & obtained within 12 hours
Forwarded to Google with "exigent circumstances"

20 minutes later Google called back

InZeit Excellence in Acuity

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

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

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

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

Located in Kentucky. Kentucky police arrested suspect after chase. Identified second suspect.

5 Days from crime report to arrest.

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

Issues:

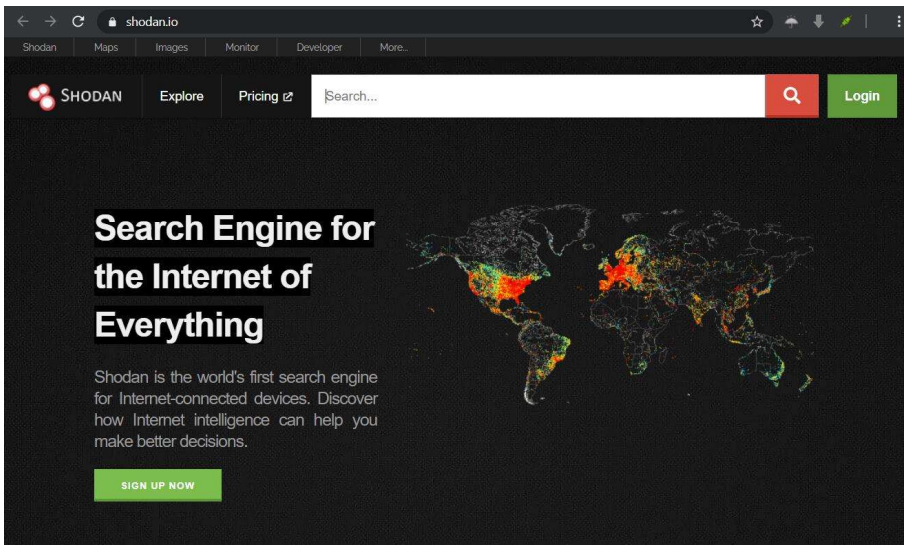
Privacy
Users 'give permission' for their phones to be tracked
The data exists, but is anonymised
Google acts as gatekeeper.

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

March 2020 Cyclist wrongly linked to a burglary because of fitness tracker on phone

https://www.theverge.com/2020/3/7/21169533/florida-google-runkeeper-geofence-police-privacy

InZeit Excellence in Acuity



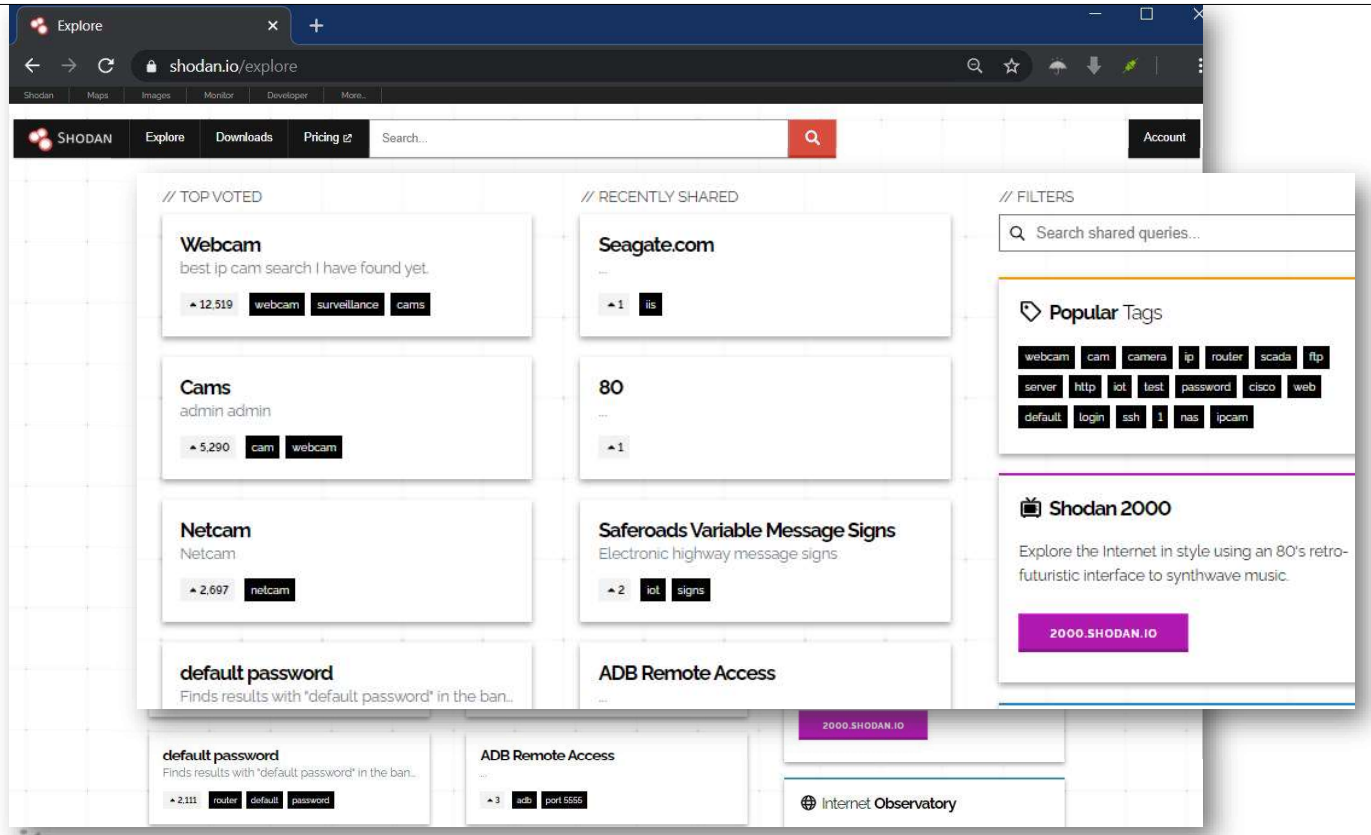
Shodan.io

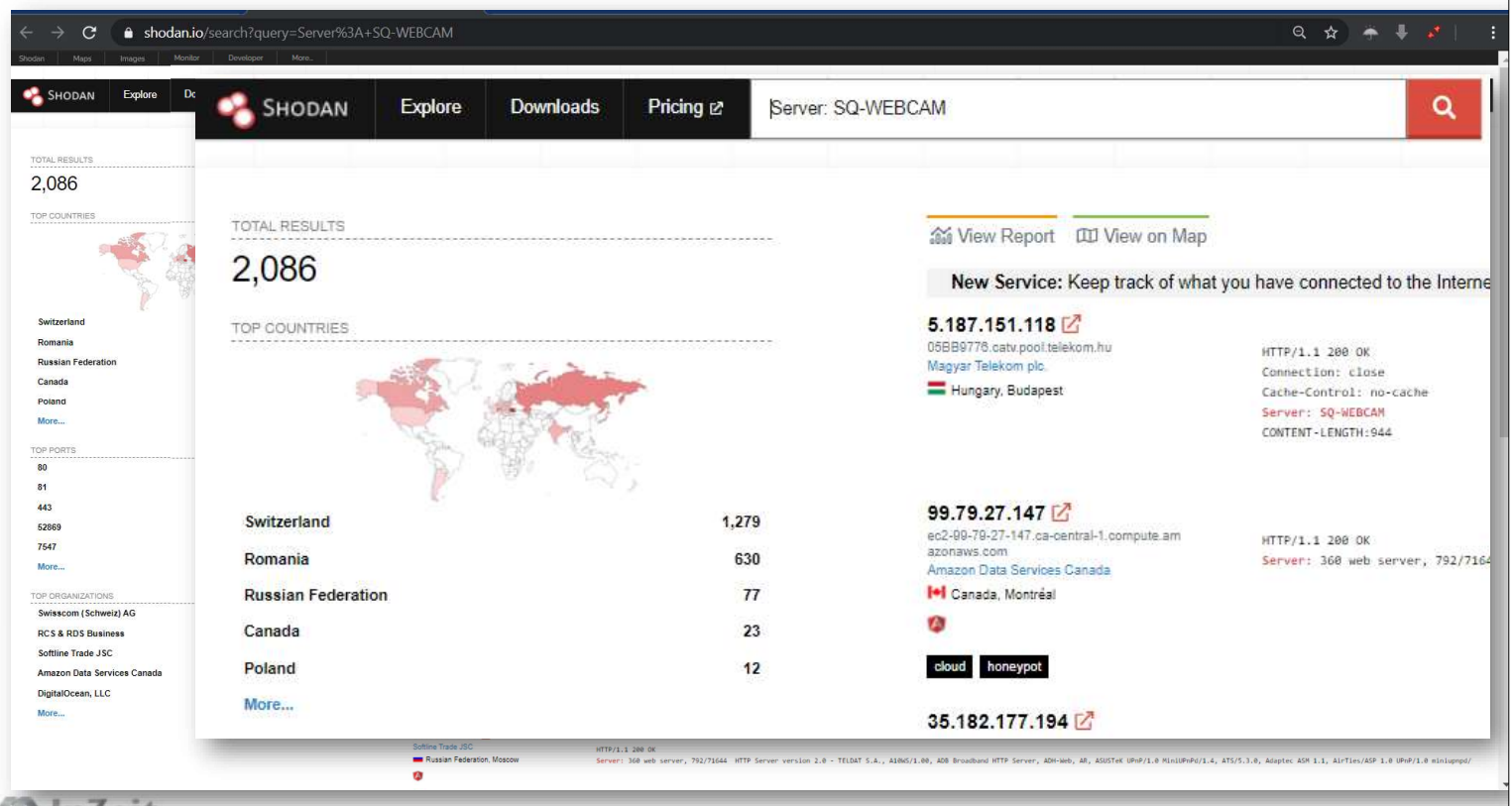
https://www.cybrary.it/video/shodan-demo/

https://www.youtube.com/watch?v=ty2cUeiAcdY

https://www.youtube.com/watch?v=v2EdwgX72PQ

InZeit Excellence in Acuity





A few 'things'

InZeit
Excellence in Acuity

Faking evidence with a bodycam

- **Officer Richard Pinheiro (Baltimore police)**
- **30 sec pre-activation recording**
- **Video shows**
  - **hiding drugs**
  - **walking away**
  - **returning to 'find' drugs**
- **Claimed restaging a legitimate find 'for the camera'**
- **Sentenced to prison terms of 3 years (suspended), 2 years probation, 300 hours community service.**

VIDEO:
https://www.baltimoresun.com/news/crime/bs-md-ci-body-camera-footage-20170719-story.html

InZeit
Excellence in Acuity

Smart doorbell

Dunstable, UK, 2021

01:00AM Luke Exelby watching TV in bed with his wife

Smart doorbell sends alert to his phone someone trying to break-in.

Intruder fled by time Luke got down stairs.

Luke contacted the police, who sent a forensics team.

Smart doorbell footage saved to remote server
Footage shared with police

"Because we got a picture of the person's face, and exactly where he put his hands on the door, they had his fingerprints. They could link his face and his fingerprints to the burglaries around the corner. They caught him straight away."

2017 Suffolk County UK, Smart doorbell recorded prolific burglar trying to break into a house.

Owner was away, but phone alert meant she watched it happening. Clear image led to his arrest and guilty plea.

Ring (smart doorbell manufacturer) donated doorbells to Suffolk Constabulary to distribute in areas of high crime.

January 2021 , Corey Rice, 19, pleaded guilty at Sheffield Crown Court to wounding, attempted robbery and possession of a blade. Recorded stabbing a man on his doorstep trying to steal gold bracelet.

https://www.theguardian.com/lifeandstyle/2021/jun/26/i-spy-are-smart-doorbells-creating-a-global-surveillance-network

Beat Nick

Ohio September 2016 Ross Compton (59)

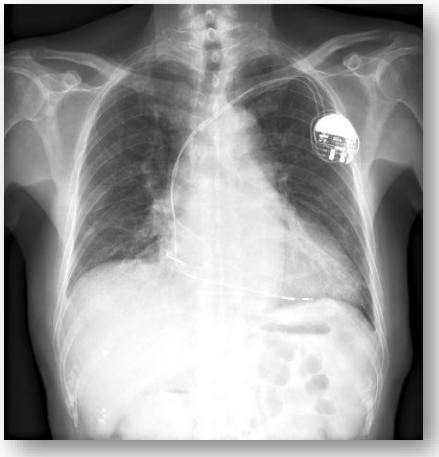
'Awoke from sleep 'to see his house on fire
He packed his bags, grabbed his computer, broke the bedroom window with his cane, threw out his belongings

Climbed out and dragged them to his car.

The fire caused US$ 400K damage and killed the cat

InZeit Excellence in Acuity

https://www.wired.com/story/your-own-pacemaker-can-now-testify-against-you-in-court/



Quite a feat
– Compton was fitted with an external heart pump

Fire investigators found fire started in multiple places and smelt of gasoline

Police obtained a search warrant and downloaded the records from his pacemaker as well as historical records from the hospital

Charged with arson and attempted insurance fraud. Compton died in hospital awaiting trial.

InZeit Excellence in Acuity

https://www.wired.com/story/your-own-pacemaker-can-now-testify-against-you-in-court/

Fitbit

8 September 2018 Santa Clara, California

Karen Navarra (67) didn't turn up for work.

She's found slumped in a chair at her dining table, large kitchen knife in her hand, her throat slit twice and head wounds from a blunt instrument.

The throat wounds were post-mortem

InZeit Excellence in Acuity

https://www.sfchronicle.com/crime/article/Murder-defendant-dies-A-Fitbit-device-linked-14432677.php

Her fitbit showed a spike in her heart rate at 15:20, then her heart rate slowed and stopped at 15:28

Her stepfather, Tony Aiello (90) said he'd passed by to bring her a pizza and left after 15 minutes

Neighbour's CCTV showed Aiello's car at the premises at least between 15:12 -15:33

Aiello died in prison in 2019 awaiting trial for her murder.

InZeit Excellence in Acuity

https://www.sfchronicle.com/crime/article/Murder-defendant-dies-A-Fitbit-device-linked-14432677.php

Smart Phones & Watches

Caroline Crouch, Athens 11 May 2021

Husband said, three armed robbers broke into their house, strangled his wife in front of their baby daughter and got away with valuables and £10,000 cash

BUT:

Timings on e-devices did not match.

InZeit Excellence in Acuity

https://greekreporter.com/2021/06/18/how-police-unraveled-murder-caroline-crouch-husband/

Smart Phones & Watches

Text argument between them on smartphones at about midnight Caroline had searched for a hotel

Caroline's smartwatch showed her asleep at 03:58 AM. At 04:05 her heartbeat was racing. She was dead by 04:11 AM

3 hours earlier memory card from home's CCTV had been removed (husband said the robbers took it when they left)

Husband's smartphone app indicated movement at time he was supposed to be tied up by the robbers

18 June Husband charged with her murder after he confessed.

https://www.vice.com/en/article/akg7ne/caroline-crouch-husband-confesses-to-murdering-wife-as-smartwatch-data-exposes-his-cover-up

InZeit Excellence in Acuity

https://greekreporter.com/2021/06/18/how-police-unraveled-murder-caroline-crouch-husband/

Arkansas 2015 James Bates charged 1st Degree Murder (later dropped on prosecutor's application). Bates gave Amazon permission to share records.

Farmington, New Hampshire 2017 Timothy Verrill accused of murdering Christine Sullivan and Jenna Pellegrini (mistrial in 2019. Motion to dismiss charges now pending).

Hallandale Beach, Florida 2019 Adam Crespo charged with 2nd degree murder of girlfriend Sylvia Galva (spear pierced chest).

Haven't found a case where Alexa/Smart Speaker evidence has led to a conviction

Virtual Assistants

InZeit Excellence in Acuity

Dilemma:

More and more devices capable of holding evidence

Do investigators seize absolutely everything??

Do you triage and hope you've everything you need (culpatory and ex-culpatory)?

Digital data overload: hours, days and weeks of specialist examination
Too few forensic facilities
Very high cost

Who 'carries the can' when a case goes wrong?

InZeit Excellence in Acuity

Kept in the dork

Google search operators

Refining & focusing your searches
(full list in links at the end)

Google may get suspicious and ask you to confirm you are human

InZeit
Excellence in Acuity

site:era.int
Limits search to given website

This AND That
Returns pages with both This AND that

This OR that
Returns pages with either this or that or both

word term –keyword
- (minus) sign excludes specified keyword

cache:webpage
Finds (old) webpages stored in browser cache

InZeit
Excellence in Acuity

Searchterm filetype:pdf
Finds file of specified type

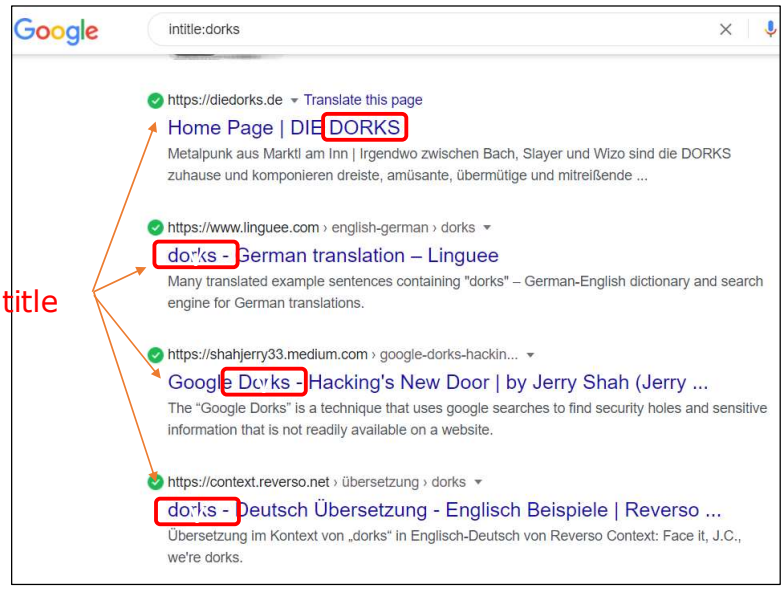
"search term"
– searches for exact phrase

John Doe (site:twitter.com | site:facebook.com | site:linkedin.com)
Search for someone's social media

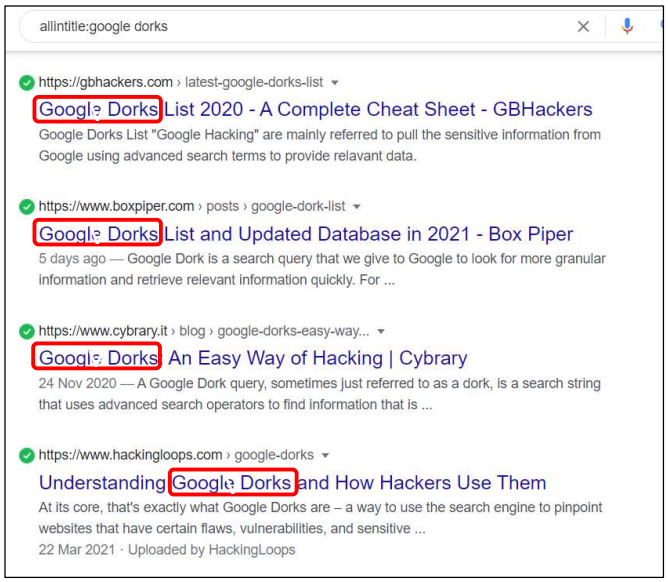
*** Can replace a missing letter, word or phrase**
e.g. * Doe

InZeit
Excellence in Acuity

intitle:**dorks**

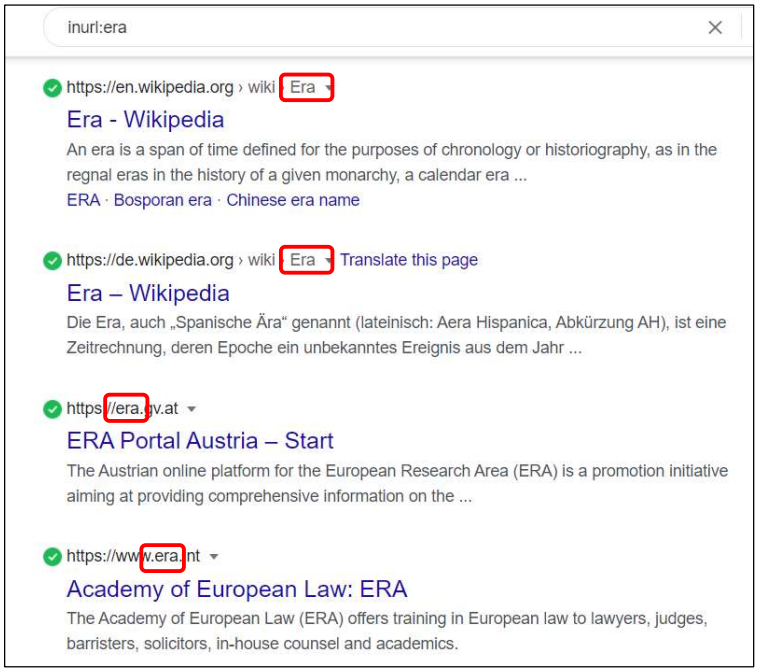


allintitle:google dorks

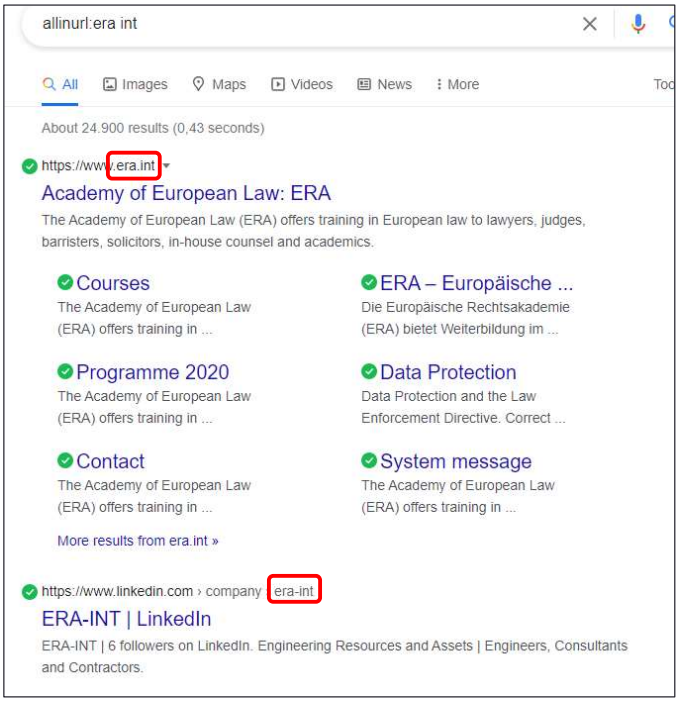


InZeit
Excellence in Acuity

inurl:era



allinurl:era int



InZeit
Excellence in Acuity

Social Media

(Patricia will focus on this later)

Platform or publisher?

Print media

Provider of paper: No liability for content

Publisher: Liable

- Curated content
- Commission writer/artist

InZeit
Excellence in Acuity

Social Media

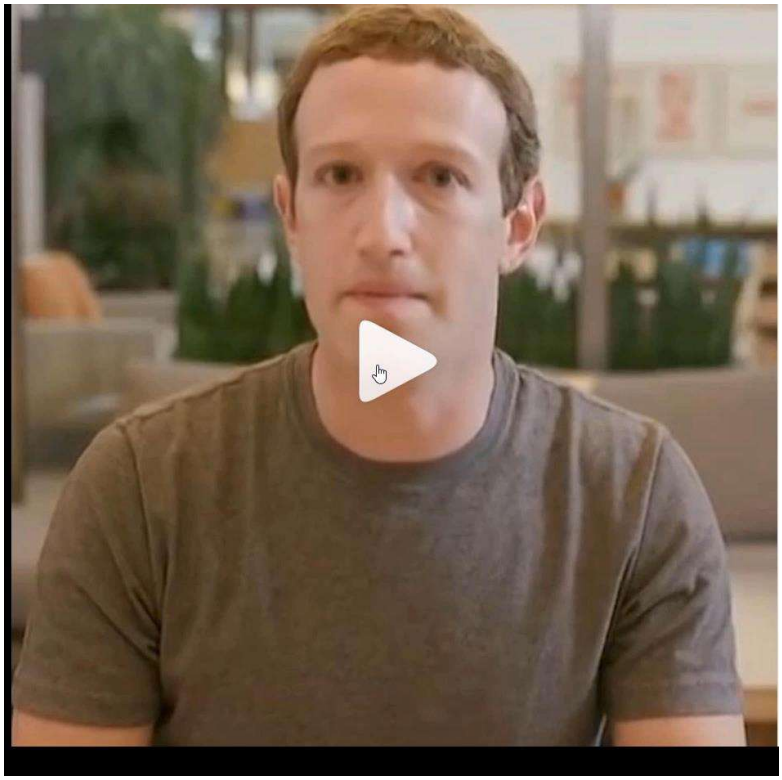
Maintain:

- They are like the paper manufacturer
- Users provide the content independently

BUT

- They 'moderate' content (human & algorithmic systems)
- Encourage content
- Use algorithms to generate 'likes'
- Generate income from the content (and usage)

https://www.ted.com/talks/james_matthews_how_the_like_button_is_shaping_your_opinions



https://www.youtube.com/watch?v=3f66kBwfMto

info(at)inzeit(dot)eu

InZeit
Excellence in Acuity

References & Further Reading

InZeit
Excellence in Acuity

CARRIER GRADE NAT

Europol (2017) Are you sharing the same IP address as a criminal? Law enforcement call for the end of Carrier Grade NAT (CGN) to increase accountability online
https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online

PRACTICAL GUIDE FOR REQUESTING E-EVIDENCE ACROSS BORDERS
https://sherloc.unodc.org/cld/en/publications/practical-guide/practical-guide.html

SHODAN Videos
https://www.cybrary.it/video/shodan-demo/
https://www.youtube.com/watch?v=ty2cUeiAcdY
https://www.youtube.com/watch?v=v2EdwgX72PQ

GEOFENCE WARRANTS

Brewster,T.(2021) 'Google Geofence Warrants Endanger Privacy—Judges Now See The Threat' https://www.forbes.com/sites/thomasbrewster/2021/06/15/google-geofence-warrants-endanger-privacy-judges-now-see-the-threat/

Cushing,T.(2021) 'Kansas Court Rejects Government's 'Reverse Warrant,' Sets Ground Rules For Future Requests' https://www.techdirt.com/articles/20210620/12123947026/kansas-court-rejects-governments-reverse-warrant-sets-ground-rules-future-requests.shtml

Davis, W.(2020) 'Law enforcement is using location tracking on mobile devices to identify suspects, but is it unconstitutional?' https://www.abajournal.com/magazine/article/law-enforcement-is-using-location-tracking-on-mobile-devices-to-identify-suspects-geofence

Green,S.J.(2021) Two men charged with murder in 2020 gang-related shooting in Federal Way https://www.seattletimes.com/seattle-news/crime/two-men-charged-with-murder-in-2020-gang-related-shooting-in-federal-way/

Lyons,K.(2020) 'Google location data turned a random biker into a burglary suspect' https://www.theverge.com/2020/3/7/21169533/florida-google-runkeeper-geofence-police-privacy

Schuppe,J. (2020) 'She didn't know her kidnapper. But he was using Google Maps — and that cracked the case' https://www.nbcnews.com/news/us-news/she-didn-t-know-her-kidnapper-he-was-using-google-n1252472

INTERNET OF THINGS

ALEXA
https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/?itid=lk_inline_manual_22

https://www.theguardian.com/us-news/2019/nov/01/alexa-florida-death-witness-amazon-echo

https://www.washingtonpost.com/technology/2019/11/02/police-think-amazons-alexa-may-have-information-fatal-stabbing-case/

https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html

https://www.engadget.com/2019-11-02-florida-police-obtain-alexa-recordings-in-murder-case.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACZMUxW_91gi43E2TWsfTfiYHu88Euxp5UXIkI7ifnbMjtNZs1-6dI7doX2z98gYmccUCSXKfIMiByWleF_FeX_4At1Rh1UdugvQMdxDXV33Px89ug_5zpyJ4q_QfHHZVWgDqUDOZWjDPRKpIxE2P1heZHmSTe7G2hbYAB6fRseJ

KEPT IN THE DORK

https://ahrefs.com/blog/google-advanced-search-operators/
https://moz.com/learn/seo/search-operators
https://www.spyfu.com/blog/google-search-operators/

BODYCAMS
https://www.baltimoresun.com/news/crime/bs-md-ci-body-camera-footage-20170719-story.html

SMART DOORBELLS
https://www.theguardian.com/lifeandstyle/2021/jun/26/i-spy-are-smart-doorbells-creating-a-global-surveillance-network

MEDICAL DEVICES
https://www.wired.com/story/your-own-pacemaker-can-now-testify-against-you-in-court/

Langston,F.(?) 'Top 6 Hackable Medical IoT Devices'
https://www.criticalinsight.com/resources/news/article/top-6-hackable-medical-iot-devices

FITBITS
https://www.news4jax.com/news/2016/02/23/fitness-tracker-data-used-in-court-cases/

https://www.npr.org/2018/01/29/581674890/former-special-ops-agent-discusses-how-tech-fitness-trackers-affect-the-military?t=1624795750522

https://www.sfchronicle.com/crime/article/Murder-defendant-dies-A-Fitbit-device-linked-14432677.php

BROWSER FINGERPRINTING

clickclickclick.click

https://www.ionos.com/digitalguide/online-marketing/web-analytics/browser-fingerprints-tracking-without-cookies/

https://coveryourtracks.eff.org/learn

https://www.researchgate.net/publication/332873650_Browser_Fingerprinting_A_survey

webkay.robinlinus.com

SOCIAL MEDIA

Greene, D.(2020) '**Publisher or Platform? It Doesn't Matter**'
https://www.eff.org/deeplinks/2020/12/publisher-or-platform-it-doesnt-matter

Matthews, J. (2017) 'How the like button is shaping your opinions'
https://www.ted.com/talks/james_matthews_how_the_like_button_is_shaping_your_opinions

DEEPFAKES

Zuckerberg DeepFake
https://www.youtube.com/watch?v=3f66kBwfMto

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

ERA Prague 2021

OPEN SOURCE TOOLS, COMPUTER FORENSICS IN THE "CLOUD"

1

Petar Majić

- FPZ - mag. ing. traff.
- Digital Forensics Consultant in INsig2 Ltd.

2

About INsig2

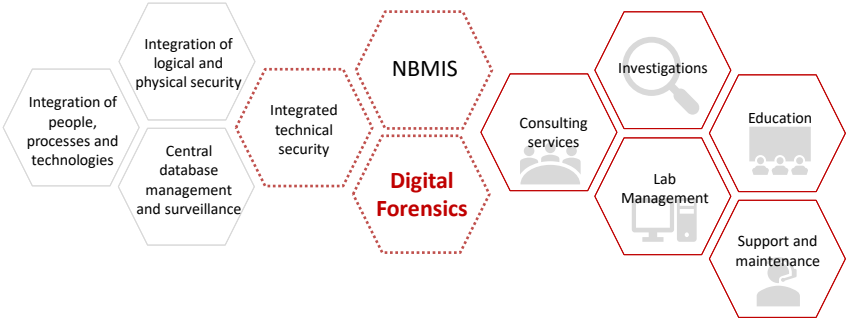
- Established in 2004, HQ in Zagreb
- 2018 INsig2 business expansion in Indonesia
- 50+ highly educated employees
- Educational & Training centre

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

3

INsig2

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



4

INsig2 Trainings

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

INSIG2

5

Clients

Abbott · aztn · ETIHAD AIRWAYS · EUROPOL · HNB · Pfizer Hospira · INTERPOL · Microsoft · Republika Makedonija Ministerstvo za finansii · Republic of Macedonia Ministry of Finance · RH MUP · NATO OTAN · OLAF European Anti-Fraud Office · Ministry of Interior Kingdom of Saudi Arabia

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

INSIG2

6

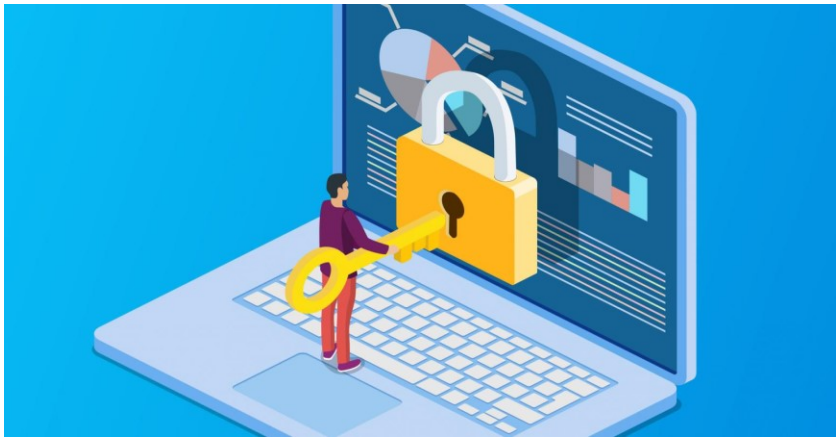
Partners

SUMURI Forensics Simplified
TEELtechnologies Canada
AMPED SOFTWARE
AccessData
Belkasoft forensics made easier
TEELtechnologies Europe
paraben corporation
Digital Intelligence
IACIS The International Association of Computer Investigative Specialists
BlackBag TECHNOLOGIES
mh SERVICE GmbH
OXYGEN FORENSICS Helping good people to make this world safer
TABLEAU
Guidance SOFTWARE
nuix
MSAB
Cellebrite
MAGNET FORENSICS
ELCOMSOFT PROACTIVE SOFTWARE

INSIG2

7

Encryption



INSIG2

8

What is Encryption?

- A security method used to protect data

- Encryption: coding text
- Decryption: decoding text

Why Do We Use Encryption?

- To secure important information e.g. :
  - Credit card information
  - Network traffic
  - Data in general
  - Etc.

- Prevents information from getting stolen or read
- Without encryption, there is no reliable security

Types of encrypted evidence

- Stored Passwords - Browsers and Password Managers
- Files, Documents - Office, PDF, Archives, Mobile Backups
- Full Disk Encryption - FileVault2, BitLocker, TrueCrypt…

INSIG2

11

Terminology

Plaintext

Original message

Algorithm

- Method how to change plaintext

Key

- Piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher

Cipher Text

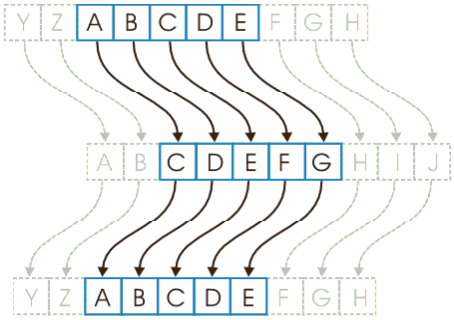
- Scrambled message

INSIG2

12

How does it work?

- Encryption allows the sender to transform data from **plain text** into **ciphertext** by using a **key**



13

Two sides to encryption

- The bad
  - Data is inaccessible to law enforcement
  - Criminal usage
  - Hard to recover if keys are lost or unobtainable
  - Everything is becoming more and more encrypted
  - Ransomware
- The good
  - Makes our data secure
  - Makes our connections secure
  - Low chance of data theft
  - Privacy and security aspects
  - Data validation

14

Dealing with encryption

- What can law enforcement do against encryption?
  - Tools for detection
  - Doing a RAM dump on a live system to get the key
  - Live acquisition if file/drive is open/mounted before evidence seizure or pulling the plug
  - Get information about the suspect and use it for dictionary attack against encrypted data
  - Speak to vendor or system administrator

INSIG2

15

Reverse image search

INSIG2

16

Reverse image search

- Is a search engine technology based on **Content-based image retrieval** (CBIR), that takes an image file as input query and returns results related to the image
- In OSINT investigation, pictures and general media are extremely powerful!
- What can be found by using reverse image search?

17

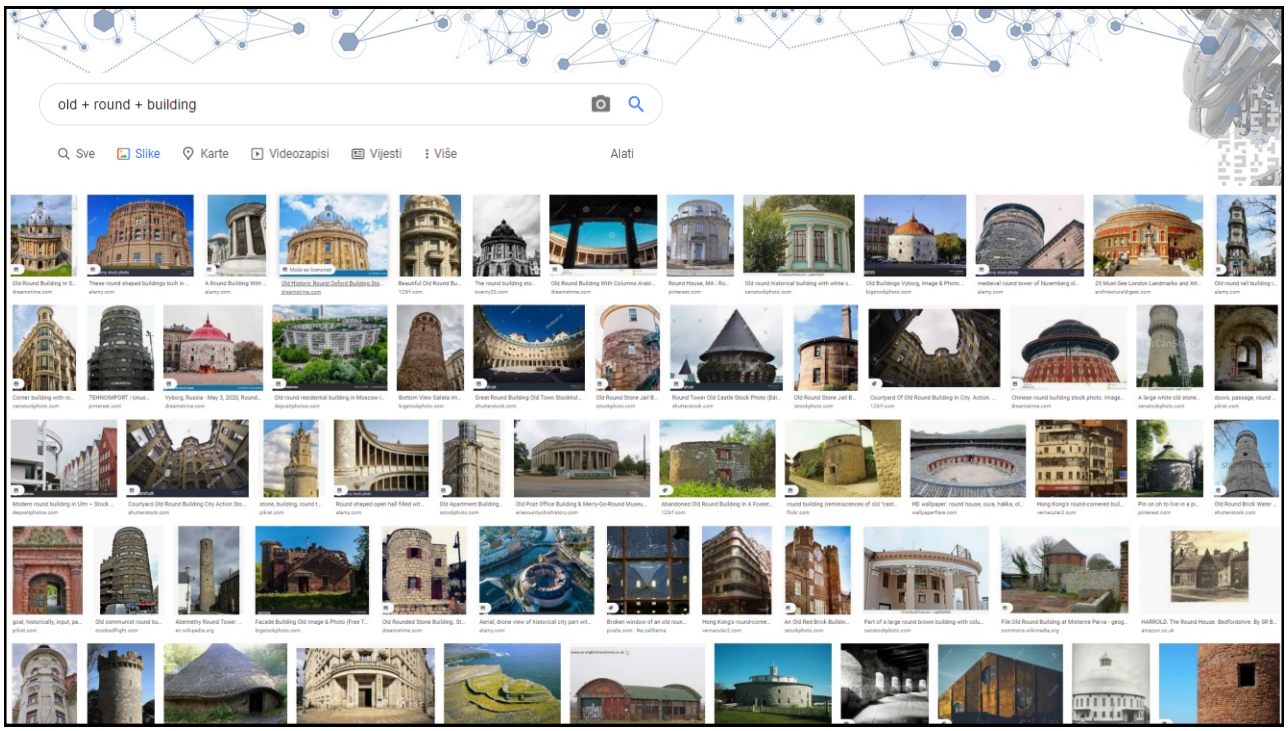
Reverse image search

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

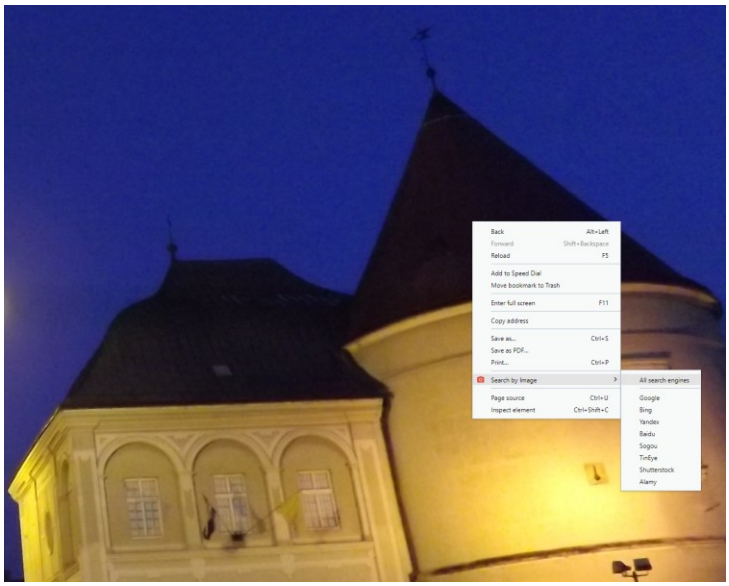
18

Reverse image practical

19



20


Back Alt+Left
Forward Shift+Backspace
Reload F5
Add to Speed Dial
Move bookmark to Trash
Enter full screen F11
Copy address
Save as... Ctrl+S
Save as PDF...
Print... Ctrl+P
Search by Image
Page source Ctrl+U
Inspect element Ctrl+Shift+C
All search engines
Google
Bing
Yandex
Baidu
Sogou
TinEye
Shutterstock
Alamy

21

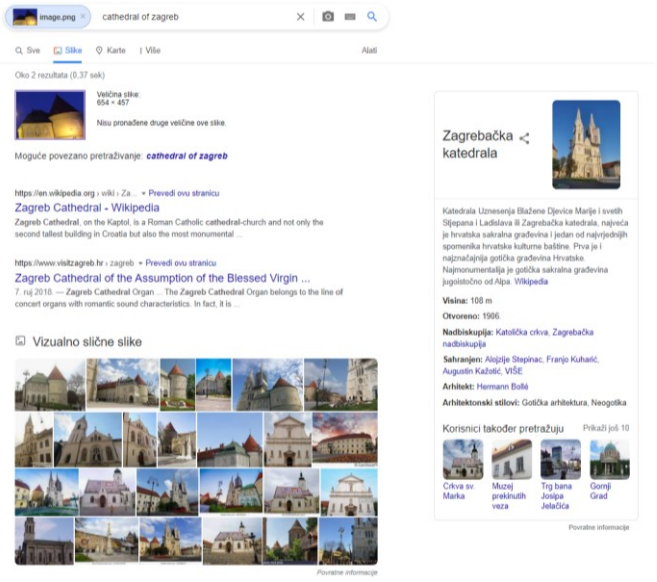


image.png
cathedral of zagreb
Sve
Slike
Karte
Više
Alati
Oko 2 rezultata (0,37 sek)
Veličina slike:
654 × 457
Nisu pronađene druge veličine ove slike.
Moguće povezano pretraživanje: cathedral of zagreb
https://en.wikipedia.org › wiki › Za... Prevedi ovu stranicu
Zagreb Cathedral - Wikipedia
Zagreb Cathedral, on the Kaptol, is a Roman Catholic cathedral-church and not only the second tallest building in Croatia but also the most monumental ...
https://www.visitzagreb.hr › zagreb Prevedi ovu stranicu
Zagreb Cathedral of the Assumption of the Blessed Virgin ...
7. ruj 2018. — Zagreb Cathedral Organ ... The Zagreb Cathedral Organ belongs to the line of concert organs with romantic sound characteristics. In fact, it is ...
Vizualno slične slike
Povratne informacije
Zagrebačka katedrala
Katedrala Uznesenja Blažene Djevice Marije i sveti Stjepana i Ladislava ili Zagrebačka katedrala, najveća je hrvatska sakralna građevina i jedan od najvrjednijih spomenika hrvatske kulturne baštine. Prva je i najznačajnija gotička građevina Hrvatske. Najmonumentalija je gotička sakralna građevina jugoistočno od Alpa. Wikipedia
Visina: 108 m
Otvoreno: 1906.
Nadbiskupija: Katolička crkva, Zagrebačka nadbiskupija
Sahranjen: Alojzije Stepinac, Franjo Kuharić, Augustin Kažotić, VIŠE
Arhitekt: Hermann Bollé
Arhitektonski stilovi: Gotička arhitektura, Neogotika
Korisnici također pretražuju
Prikaži još 10
Crkva sv. Marka
Muzej prekinutih veza
Trg bana Josipa Jelačića
Gornji Grad
Povratne informacije

22

EXIF data

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

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

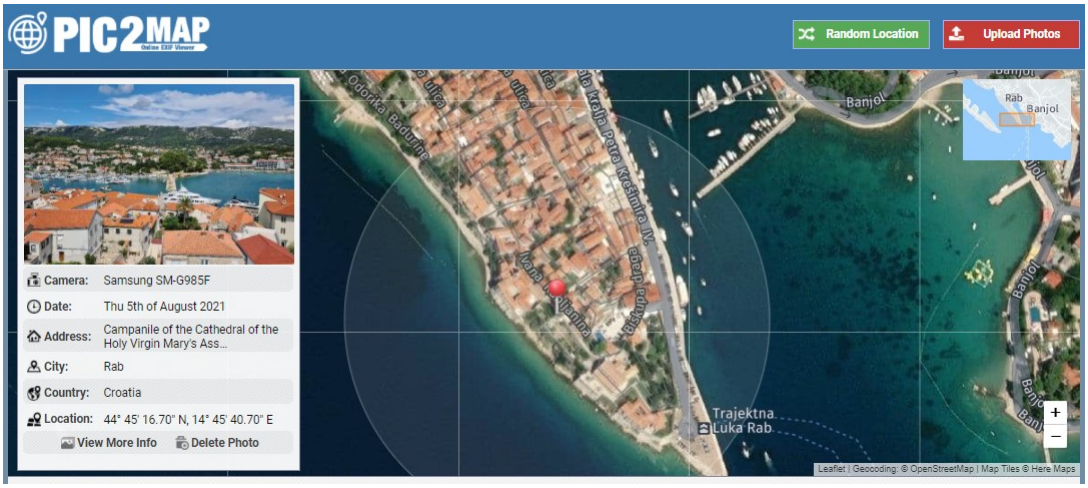
23

Exercise (EXIF data analysis)

- Use Pic2map website to find information:
  - 20210805_143559.jpg

24

Pic2map results



25

Pic2map results

CAMERA INFORMATION

Brand: Samsung	Model: SM-G985F	Lens Info: Unknown
Shutter: 1/1488 (0.0007 seconds)	F Number: f/2	ISO Speed: ISO 25
Flash: Not Used	Focal Length: 5.9 mm	Color Space: RGB

FILE INFORMATION

File Name: 20210805_143559.jpg	Image Size: 9248 x 6936 pixels	Resolution: 64.1 megapixels
Unique ID: R64LLMF05VM	MIME Type: image/jpeg	Dots/Inch: 72 DPI

DATE & TIME

Date: 2021-08-05	Time: 14:36:00 (GMT +02:00)	Time Zone: Europe / Ljubljana

GPS INFORMATION

Latitude: 44.754640	Longitude: 14.761304	Lat Ref: North
Long Ref: East	Coordinates: 44° 45' 16.70" N , 14° 45' 40.70" E	Altitude: 0m. (Above Sea Level)
Direction Ref:	Direction:	Pointing:

LOCATION INFORMATION

City: Rab	State: Rab	Country: Croatia

26

Jimpl.com

Aperture	2.0	FNumber	2.0	ImageHeight	6936
ApertureValue	2.0	FOV	67.4 deg	ImageSize	9248x6936
BitsPerSample	8	FileAccessDate	2021-09-28 15:48:24 +0300	ImageUniqueID	R64LLMF05VM
BrightnessValue	25.28	FileInodeChangeDate	2021-09-28 15:48:24 +0300	ImageWidth	9248
CircleOfConfusion	0.007 mm	FileModifyDate	2021-09-28 15:48:24 +0300	LightValue	14.5
ColorComponents	3	FilePermissions	prw-------	MIMEType	image/jpeg
ColorSpace	sRGB	FileSize	0 bytes	Make	samsung
Compression	JPEG (old-style)	FileType	JPEG	MaxApertureValue	2.0
CreateDate	2021-08-05 14:36:00 +0300	FileTypeExtension	jpg	Megapixels	64.1
DateTimeOriginal	2021-08-05 14:36:00 +0300	Flash	No Flash	MeteringMode	Center-weighted average
DigitalZoomRatio	1	FocalLength	5.9 mm	Model	SM-G985F
EncodingProcess	Baseline DCT, Huffman coding	FocalLength35efl	5.9 mm (35 mm equivalent: 27.0 mm)	ModifyDate	2021-08-05 14:36:00 +0300
ExifByteOrder	Little-endian (Intel, II)	FocalLengthIn35mmFormat	27 mm	OffsetTime	+02:00
ExifImageHeight	6936	GPSLatitude	44 deg 45' 16.70" N	OffsetTimeOriginal	+02:00
ExifImageWidth	9248	GPSLatitudeRef	North	Orientation	Horizontal (normal)
ExifVersion	0220	GPSLongitude	14 deg 45' 40.70" E	ResolutionUnit	inches
ExposureCompensation	0	GPSLongitudeRef	East	ScaleFactor35efl	4.6
ExposureMode	Auto	GPSPosition	44 deg 45' 16.70" N, 14 deg 45' 40.70" E	SceneCaptureType	Standard
ExposureProgram	Program AE	HyperfocalDistance	2.65 m	ShutterSpeed	1/1488
ExposureTime	1/1488	ISO	25	ShutterSpeedValue	1

27

Is it possible to see offline website?

28

How to review a webpage or site that is offline

29

Offline website?

- There are cases when you can't access the website
- There can be several reasons:
  - Your IP
  - Organization restriction
  - Location
  - Site is offline

30

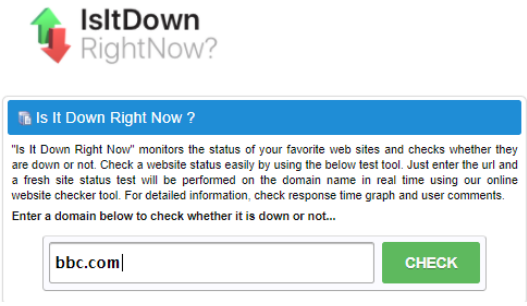
How to check if the site is up?

- By using several free tools we can check if the site is online or offline

- Tools
  - https://www.isitdownrightnow.com
  - https://www.websiteplanet.com/webtools/down-or-not/
  - https://www.host-tracker.com
  - https://www.site24x7.com/check-website-availability.html

31

isitdownrightnow



32

Wayback Machine

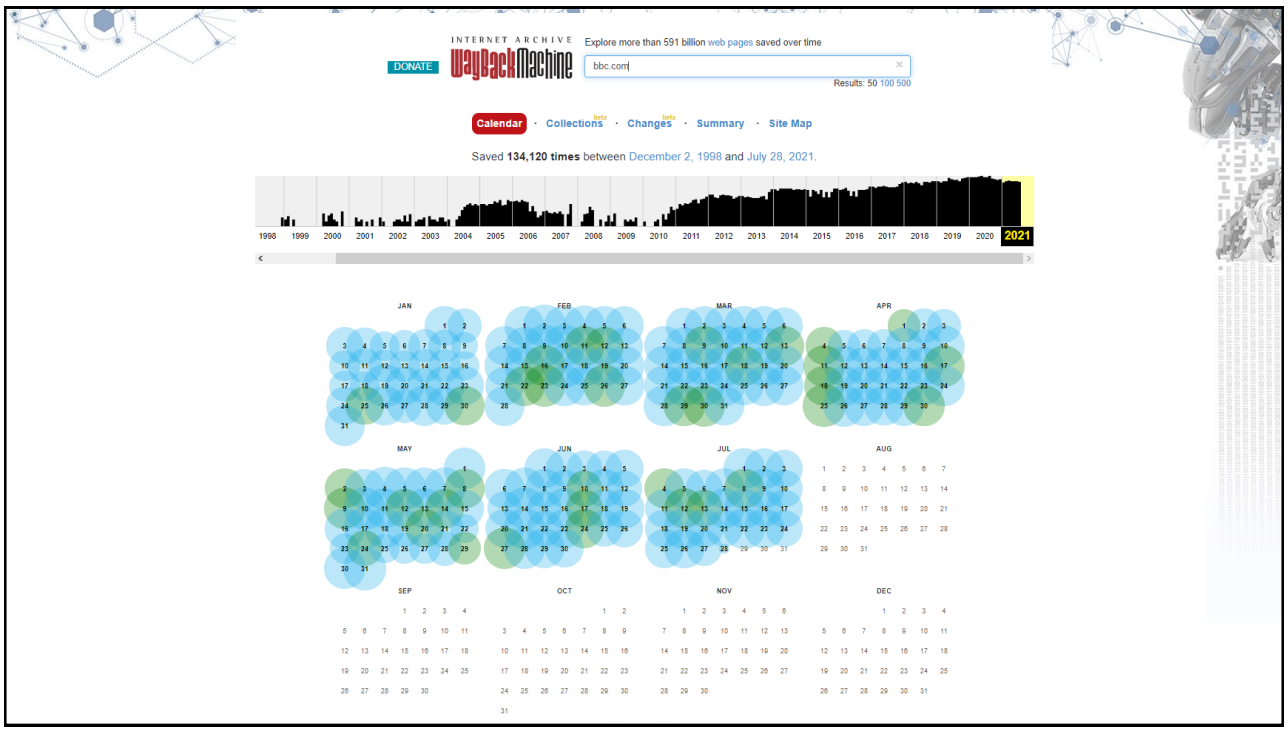
- We can use Wayback Machine to see website snapshosts from the past
- Wayback Machine is a digital archive of the World Wide Web
- Over 500 000 000 000 pages in archive

- Wayback Machine alternatives: **archive.today, Perma.cc, Pagefreezer…**

INTERNET ARCHIVE
WayBackMachine

INSIG2

33



34

Other useful tools

- OutWit Hub
- OSIRT
- Lumen
- Spiderfoot
- Hunchly
- FOCA

Physical and logical acquisition of data

37

Data acquisition

- **Retrieving evidence data from various types of media**
- Acquisition tools
  - software (forensic imaging programs)
  - hardware (write blockers, forensic duplicators, other forensic devices)
- Validation is necessary
- Destination media

38

Data acquisition

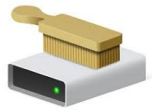
- Acquisition software
  - EnCase, X-Ways, FTK Imager, Linux forensic distribution
  - Pre - and post-acquisition hash → Verifying evidence integrity
  - Generating forensic copies and image files
- Mounting images
  - Images can be mounted as physical devices and assigned a drive number in Device Manager
  - Running a live operating system off a forensic image

39

Sterile media

- As we know, even after deleting files there is leftover data
- If destination disks for forensic backups contain leftover data from earlier, it could be mistaken for evidence

  → Sterile media
- Sterile media has every byte overwritten with a known or random hex value
- Forensically sterile media → Every byte has the value of **0x00**
- Sterilization = wiping



40

Physical image

- Physical image:
  - Will capture all ones and zeroes on a drive
  - It will create an identical copy of the source drive
  - Contains free space of the drive
  - Allocated + unallocated space is imaged
  - **Captures deleted files and fragments of a drive** (even of it was recently formatted)
  - Takes a long time
  - 1TB of source drive requires the same or more free space on the destination drive

INSIG2

41

Logical image

- Logical image:
  - Will capture all active data (the same as using File Explorer)
  - Captures only allocated space on the disk
  - Does not capture deleted files or free space
  - If imaging a 1TB drive that only has 30GB of active data/files, the destination drive will only need 30GB
  - Images can be created very fast

INSIG2

42

Cloud providers and replicated data on websites and social media

43

Cloud forensics

Cloud forensics is the application of digital forensic science in cloud environment

44

Cloud forensics

- Identification of potential evidence
  - Storage networking and virtualization makes mapping storage devices complex
- Acquisition
  - Not possible to access physical incident scene
  - Not physical but logical items
- Not auditable
  - Investigations on dynamic systems that can't be frozen
  - Documentation and expertise
- Virtualization layer might add time drift

INSIG2

45

Inaccessibility of data in the Cloud

- Evidence can be spread all over the world
- Decentralized logs
- Virtual instances may migrate transparently between physical instances with little recordkeeping

- Problems:
  - **ACQUISITION**: Gathering data
  - **AUTHENTICATION**: User's data kept together with other user's data on same storage system, hard to separate

INSIG2

46

Large amount of Cloud data

- Storage space
- Acquisition and processing time increased
- Lot of information to analyse

- VM instance size increases with amount of data in VM
  - To get data, VM instance image needs to be downloaded

47

Why is evidence from social networks hard to collect?

- Multimedia
  - Can contain images, videos, text, comments, likes, location coordinates…
- Infinite scrolling
  - Can scroll infinitely
- Deeplinked content
  - 30% of social media messages contain links
- Link shorteners
  - Short links (bit.ly) can change over time or expire
  - Can lead to bad places

48

48

Why is evidence from social networks hard to collect?

- Information credibility
  - Can be manipulated
  - Expert can get information but he can't be sure if the information is true
  - Possible to obtain information directly from social network
- Information sensitivity
  - Can be deleted at any time by user
- Information copying
  - Can be easily copied to storage device or saved as screenshot

Chain of custody

- One of the most vital issues in traditional digital forensic investigation
- Clearly describes how the evidence was:
  - Collected
  - Analysed
  - Preserved
- It starts with gaining physical control over evidence – in Cloud forensics, this step is not possible
- Dependence on CSP to acquire evidence raises suspicions to whole investigation process

Presentation in the court

- Final step of digital investigation
- Proving evidence from a complex structure of cloud computing – NOT EASY!
- Court members possibly have basic knowledge of personal computers

INSIG2

51

Cloud forensics challenges

- Jurisdiction
- Lack of international collaboration
- Investigating external chain of dependencies of the cloud provider
- Lack of law/regulations
- Decreased access and control over forensic data

INSIG2

52

Thank you!

petar.majic@insig2.com

INSIG2

53

Finding the needle somewhere in the internet

Dennis Pielken

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

1

Who am I?

RR, Dipl.-Ing.
Dennis Pielken

- Lecturer for Cybercrime & Digital Investigations, Rhineland-Palatinate Police University
- Expert witness for digital forensics
- Working in digital forensics and digital investigations for the last 13 years

2

Definition OSINT

What is Open Source Intelligence?

„**Targeted** information gathering from publically available sources for **reliable** information to answer an **inital question** and preserve this information for future research.“

OSINT = **O**pen **S**ource **Int**elligence

3

Example #1

Known facts: An unknown TOR-User provides a plattform in the darkweb to share and distribute child pornography.

This TOR-User has a unique username.

Based on English terms used by this user, his country of origin can be guessed.

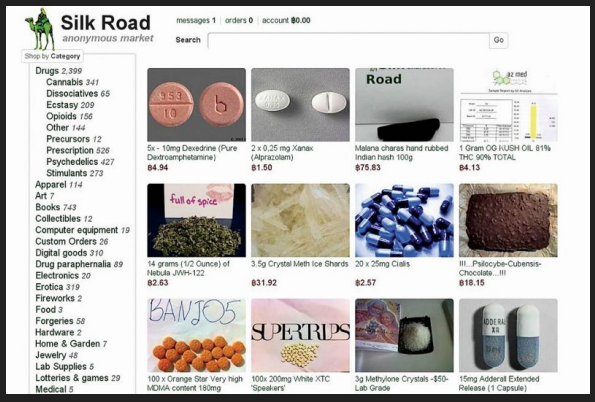
He also mentions in “public” chats that he is a passioned mountain bike cycler.

Almost the same pseudonym was used in a mountain bike community, where this user published his tracks.

User was identified based on this information using traditional Police investigation techniques.

4

What is Silkroad?



5

Example #2 Silkroad

Shortly after Silkroad went live:

3 days later

User **altoid** asked in a discussion board, what other people think of Silkroad

A user, named **altoid**, asked in another discussion board, what other people think of Silkroad

1 year later

Investigators believed that both users are the same human being.

The user **altoid** searches with a post for talented developers in the second discussion board and posts his contact email address **rossulbricht@gmail.com**

A few month later

Investigators find a social media profile page that is linked to this Email address. This social media profile page shares a lot of views with the Silkroad administrator.

6

Example #2 Silkroad – cont.

few hours later

A user **Ross Ulbricht** asks for help regarding a programming problem

The user name is changed from Ross Ulbricht to frosty and the Email address is changed to **frosty@forsty.com**

The email address *frosty@frosty.com* was also used on Silkroad by its administrator

7

OSINT: The challenges

- Managing the **information tsunami**
- How can we determine that information is **reliable**?
- How do we ***preserve*** this information / evidence?

8

Different identifier, different question

E-Mail-Addresse | Phone number | Pseudo-nym | Name

What main / initial question needs to be answered in respect to the identifier?

- E-Mail-Addresse: Where has this email addresse been used on other plattforms?
- Phone number: Is this phone number still active?

Standard search engines are not always the best starting point.

9

Identifier: Name

Question

- What kind of information are available about this person`

Starting Points

- People search engines, such as www.yasni.de, www.spokeo.com, www.pipl.com or www.northdata.de

10

Identifier: E-Mail-Addresse

Question

- Where has this email adresse been used to register an account?

Start points

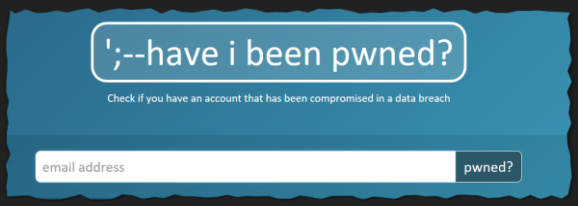
- Data leackage sites:
  - http://haveibeenpwned.com
  - https://ghostproject.fr/
  - https://dehashed.com
- Use a standard search engine, eg. google

11

Have I been pwned?

The website www.haveibeenpwned.com allows Internet users to check whether their personal data has been compromised by data breaches.

Search based on an email addresse to check, if this addresse is included in a data breach.



12

Identifier: Pseudonym

Question

- Is this username/peudonym being used on other side

Search engines

- Using one website to check, if this username exist on other sites:
  - https://namechk.com/
  - https://namecheckup.com/
  - https://knowem.com/
  - https://usersearch.org/
  - https://archive.org/details/@NAMEDESUSERS
- Search in social networks
  - (https://www.social-searcher.com/)

13

The challenge – what is reliable information

- not unique pseudonyms or names
- fake profiles for hiding
- misinformation
- „Didn‘t find anything“ means doesn‘t exit?

14

social media as a data source

What is facebook?

Users to connect with friends and family by sharing status updates, personal photos and other items of interest.

What is instagram?

photo and video sharing social networking service

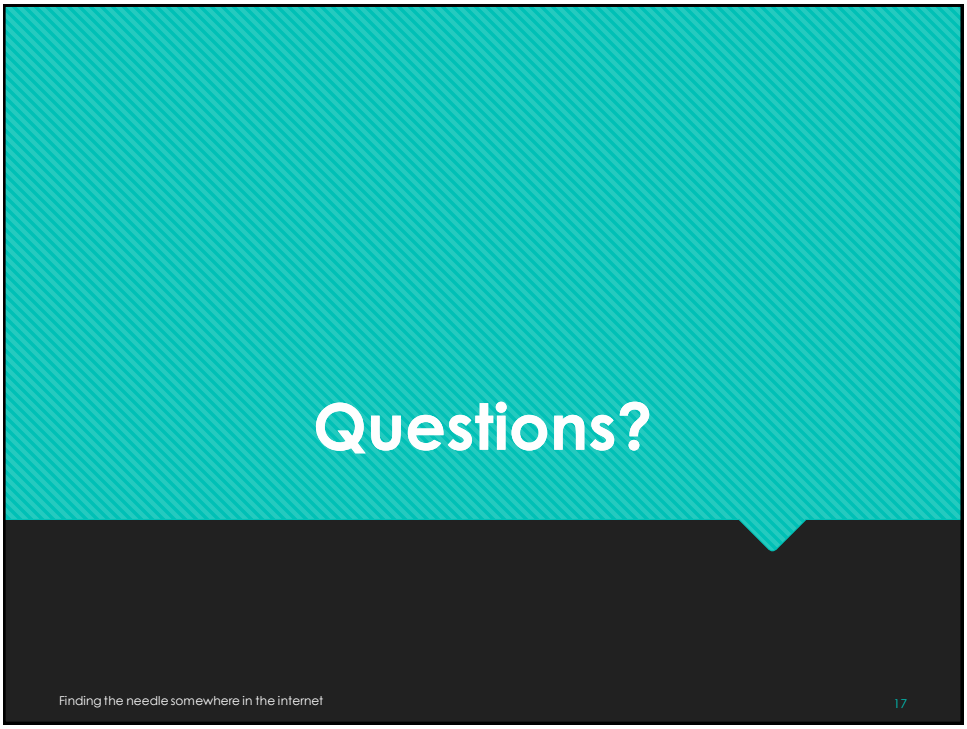
What is twitter?

Microblogging (posts limited to 280 characters) and social networking service on which users post and interact with messages known as "tweets"

15

Live Demonstration

16



17

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

University of Antwerp
Faculty of Law

Websites and social media

the legal challenges of dealing with electronic evidence in criminal proceedings

Prof. dr. Joachim Meese
associate professor
attorney

1

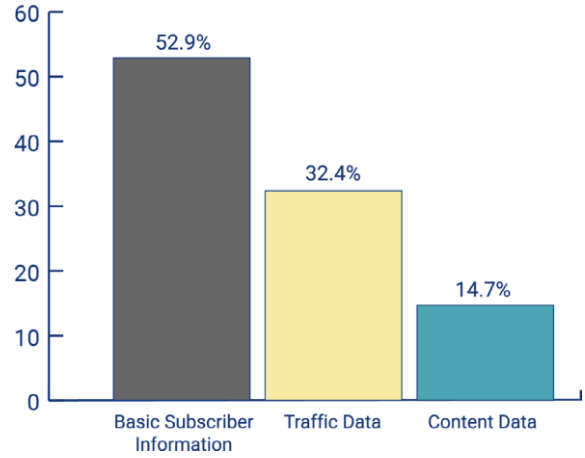
most common types of e-evidence

- **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

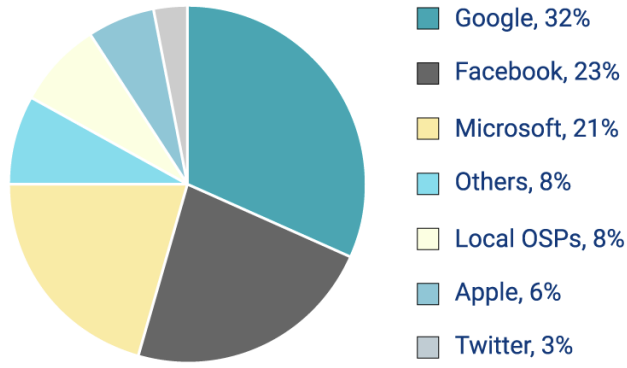
- most often needed type of e-evidence from foreign authorities or online service providers in 2019:



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

5

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)

6

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

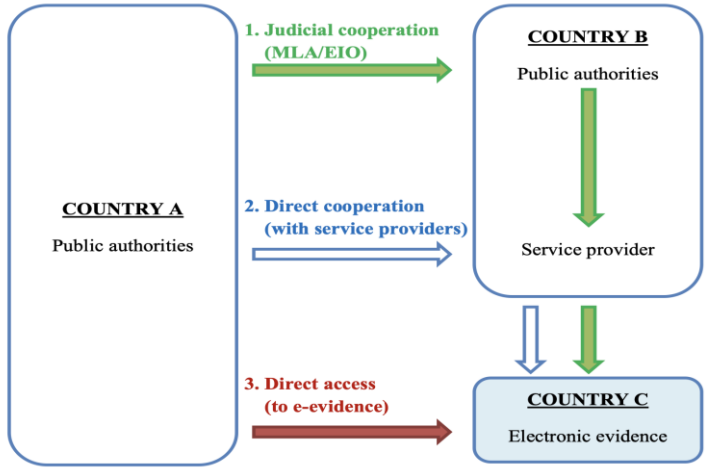
https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

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

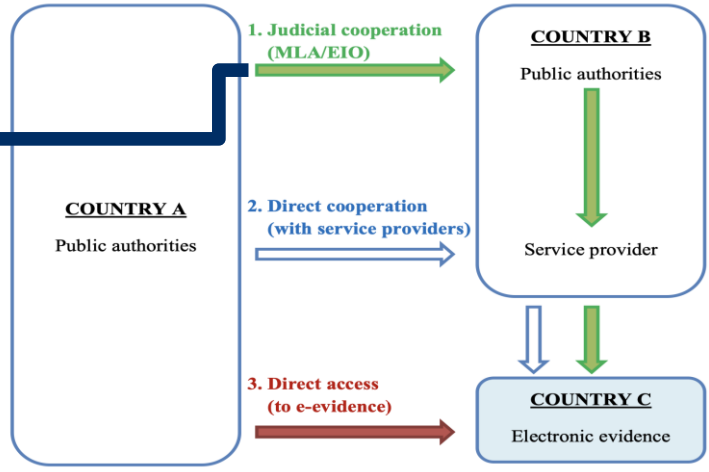
- **possible scenarios:**



cross-border access to evidence

- **possible scenarios:**

✓ within EU: EIOD
✓ outside EU: international agreements
  - Budapest Convention on cybercrime
  - 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)

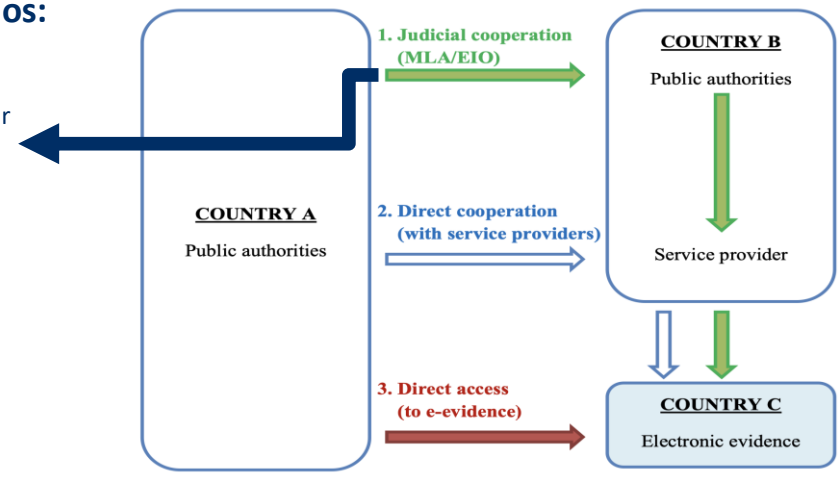


cross-border access to evidence

- **possible scenarios:**

number of requests per year on e-evidence:

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

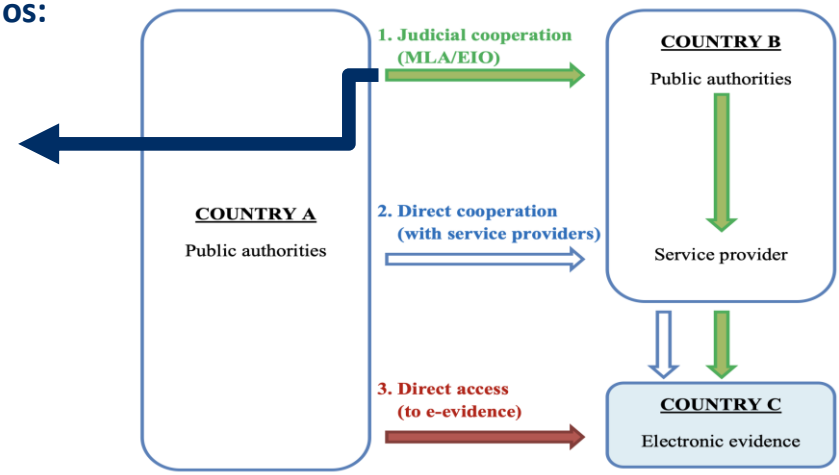


11

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

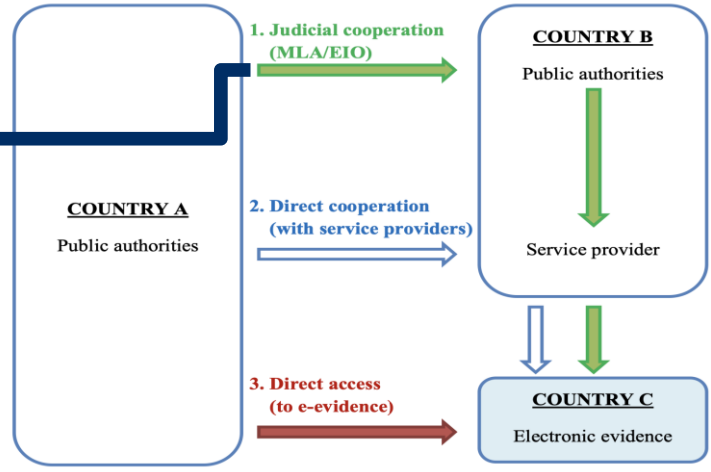


12

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

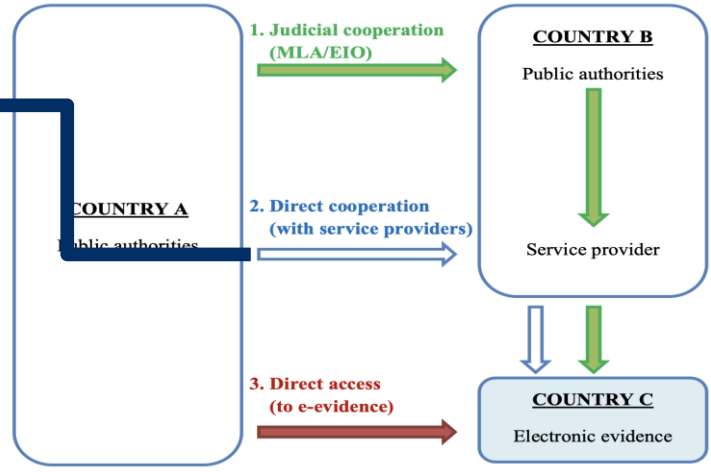


cross-border access to evidence

- **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

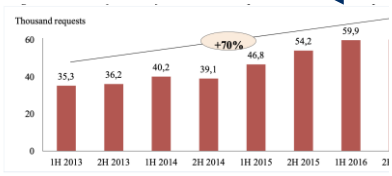
✓ WHOIS data
- service providers make data directly available to authorities through a centralised search system which does not rely on individually reviewed requests



cross-border access to evidence

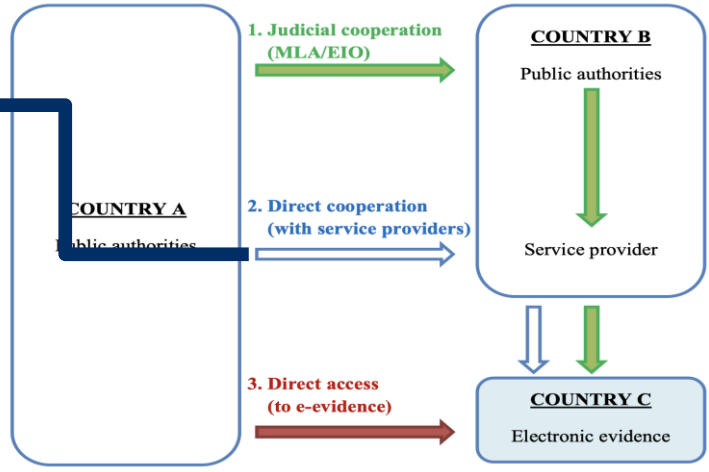
- **possible scenarios:**

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

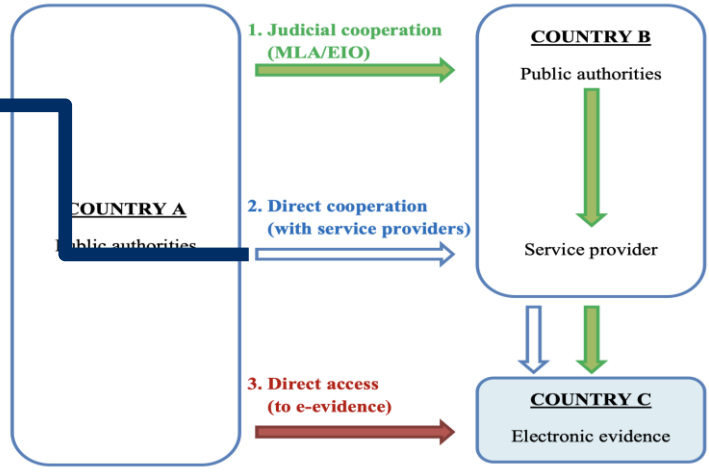
→ Google & Facebook: 70% of total requests



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)

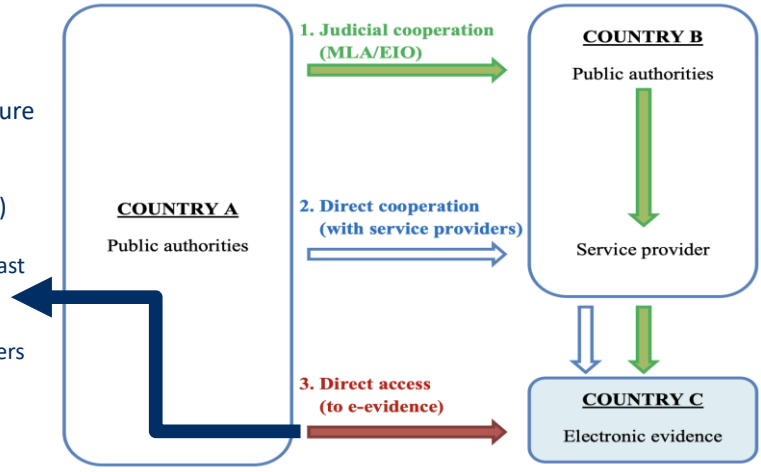


cross-border access to evidence

- **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)

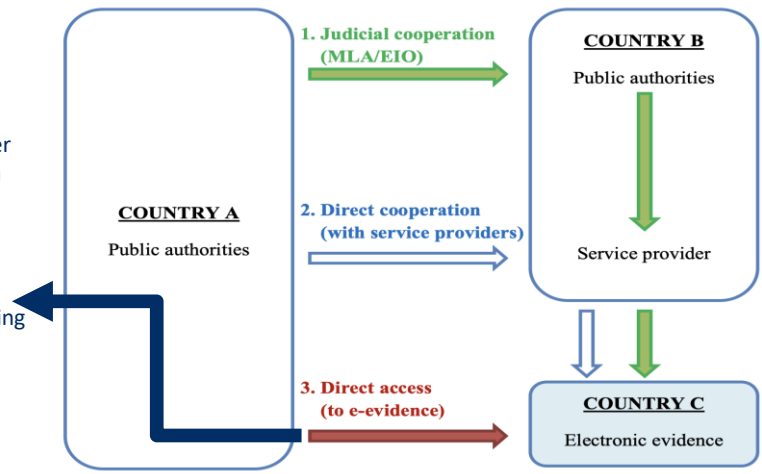


17

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: MLA, EIOD or 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: MLA, EIOD or 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
    - 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!)

Thank you!

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

University of Antwerp
Faculty of Law

23

Social media and electronic evidence

How social media networks yield digital evidence of the planning and commission of crimes, and assisted in cyber investigations resulting in the creation of solid cases against the defendants , or their acquittals

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

Patricia Ayodeji
Lawyer, England, Wales & Spain
payodeji@icab.cat
www.e-pdp.eu

Prague 18-19 October 2021

1

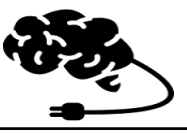
How?

Gathering valuable evidence: profiles, lists of friends, group memberships, events attended, timeline/wall/feeds posts, tweets, re-tweeting photos, videos, likes, login times etc.etc.

Organisations involved in the investigations

Central Intelligence Service against Terrorism & Organized Crime (TEPOL) Judgement No. 1

Central Section of Information Technology Crimes (SCDTI)
Case No. 4



2

Spain – Different types of police forces

Civil Guard (Guardia Civil)

Military rank. Judicial unit. Cybercrime. Counterterrorism ++

National Police (Policia nacional)

Civil rank. Judicial unit. Violent crime. Border control. Terrorism ++

Local or Municipal Police (Guardia Urbana in Catalonia)

Mostly Local Authority enforcement matters. Serious matters are handed over to either the Civil Guard or National Police

Autonomous police (Mozos de Escuadra, in Catalonia).

Demonstations etc.

3

Civil Guard

4

Civil Guard
www.gdt.guardacivil.es

TELEMATIC CRIMES GROUP (GDT)
The most specialized unit dealing with complex investigations.
Chase the crimes of glorifying terrorism in social networks
National. Teams in each of the Spanish provinces.

Interpol
G-8 for cybercrime
Europol

Other investigations dealt with by the Technological Investigation Teams (EDITEs)

5

Resources of e-Evidence

Social Media a form of e-communication : websites and apps enabling users to share content or participate in social networking

Digital Evidence any probative info. stored or transmitted in digital form over the internet or computer networks.

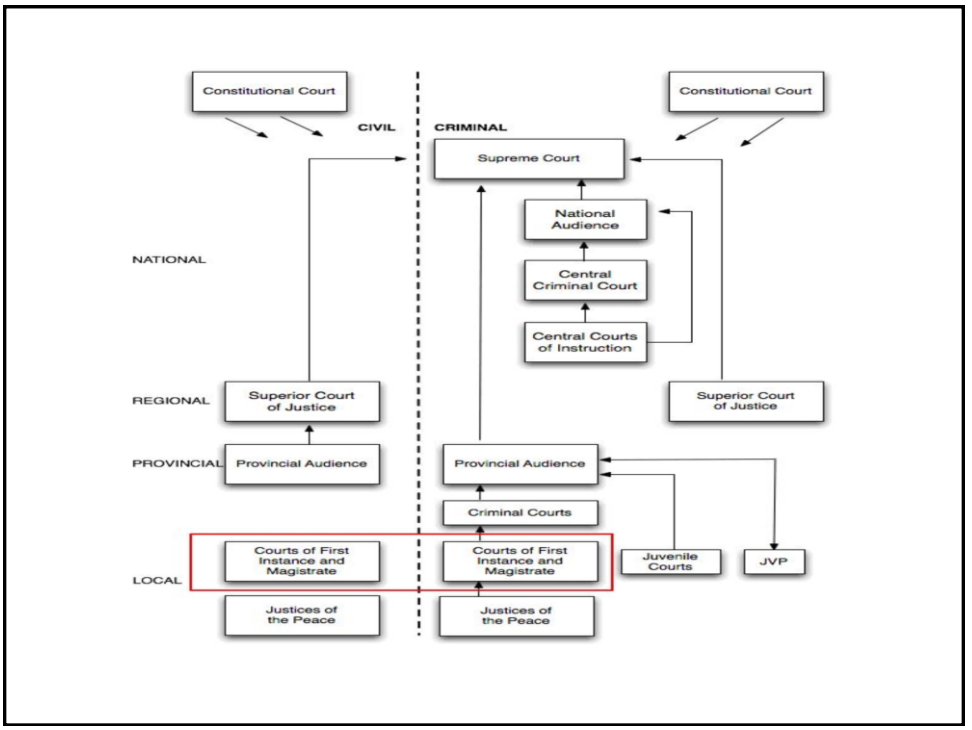
6

Lists of friends, events, groups, likes, tweets, retweets….Do they matter?

7

Spanish Courts

8


Constitutional Court
CIVIL
CRIMINAL
Constitutional Court
Supreme Court
National Audience
Central Criminal Court
Central Courts of Instruction
NATIONAL
REGIONAL
Superior Court of Justice
Superior Court of Justice
PROVINCIAL
Provincial Audience
Provincial Audience
Criminal Courts
LOCAL
Courts of First Instance and Magistrate
Courts of First Instance and Magistrate
Juvenile Courts
JVP
Justices of the Peace
Justices of the Peace

9


Spanish Court decisions Criminal Code

10

Growing number of convictions including custodial sentences.

Catch all labels?

Disproportionate restrictions to the right to freedom of expression?

11

Judgment No. 1 June 2018 – Provincial Audience (Audiencia Nacional) Madrid
Case No. 18/2018

Crime: Glorification of Terrorism

Central Intelligence Service against Terrorism & Organized Crime (TEPOL)

Citizen Reports before Civil Guard: Initially no privacy settings preventing access to profile.

Internet history. Constant accessing & viewing ,saving of terrorist material & subsequent publication in his social media profiles. High level of Internet usage.

Facebook profile logo associated with Al -Qaeda

Twitter associated with his mobile number. Al-Qaeda flag.
Whatsapp with terrorist images .

Previous conviction for murder related to terrorist groups.

12

Continued: Judgment No. 1 June 2018 – Provincial Audience (Audiencia Nacional) Madrid Case No. 18/2018

Vast volumes of digital evidence generated by mobile and computer

Purchase of **internet cards** to evade detection & browse anonymously

Internet savvy . Anonymizing Proxy Server to make IP anonymous & appear as if in different country to which he was really accessing.

Tox network for enabling anonymous communication

Whatsapp, **App Imo** – to exchange encrypted messages

Twitter – changed from public tweets to protected tweets using tools used by some marketing professionals and experts

Search warrant -House - Pendrive 158,710 terrorist group files. Hard drive: docs to make explosives. Bit2bit copy. **Convicted. 4 years** .

13

"Hell hath no fury like a woman scorned"

William Congreve (English playwright & Poet)

14

Judgment No. 2 June 2018 – Provincial Audience (Audiencia Provincial) Valladolid Case No.00184/2018

Crime: Harassment

Legality & procedural concerns of admissibility

Facebook: Threatening messages to ex
Court order- Facebook Ireland Ltd.- IP address, time line etc. Preservation of digital evidence-copy made of profile to avoid loss or destruction. Instructions not to notify profile user
Vodafone Spain – name & address of the owner of IP address. – dates & times.

Appeal against conviction - Account & User ID , Reasonable expectation of privacy violated
Authenticity of the info; prove accused was the author - IP not secure & could be intercepted by third parties, Wi-Fi.

Guilty 2 month fine of 8€ a day

15

Judgement No. 3
Supreme Court (Tribunal Supremo) Sala Segunda, de lo Penal, Judgement 72/2018
9 Feb. 2018, Rec. 583/2017

Miguel – 2 tweet accounts

Criminal code- glorification of terrorism and incitement to hatred
(women & victims of domestic violence)

@ Email of Police Unit Social Media II: control, following and analysis of content published in social media- from various citizens complaining + 2 complaints in different police stations.

Dates & content. 1 account closed by Twitter

Guilty

16

Case No. 4
Supreme Court

TRIBUNAL SUPREMO
Causa especial 20907/2017

17

***Crime*: Catalan Independence Referendum 1 October 2017 after 18 attempts to organize a Scottish-style referendum with successive Spanish Governments)ruled illegal by Spain's constitutional court – went ahead and followed by declaration of independence**

- Analysis of forensic techniques for the acquisition of digital evidence
- Acquisition, copy & analysis of computer equipment and networks
- Copy & analysis of mass storage devices or mobiles
- **Analysis of information from websites and social networks**
- IP user data to identify and locate users and computer equipment

18

II.



- Whatsapp
- Twitter
- Auto destructive SMS
- Emails
- Cloning of webpages (140) created to promote referendum - name & address of the owner of IP address (mostly with servers in the US)

19

III.

Law on the Referendum on Self-determination of Catalonia : Law that governs the holding of the Referendum of **1-O**

7 September 2017 –Law declared illegal & suspended by the Constitutional Court after a request from the Spanish government, who declared it a breach of the Spanish Constitution.

In early September High Court of Justice of Catalonia issued orders to the police to try to prevent it, including the detention of various persons responsible for its preparation.

20

IV:

1 October 2017 referendum held (referendum of **1-O)**

27 October 2017- The ruling separatists in the Catalan parliament declared independence. Madrid imposed direct rule by invoking Article 155 of the constitution - a first for Spain.

From **12 February 2019**, trial in the Supreme Court in Madrid of the Catalan Independence leaders

21

VI.

How *not* to present digital evidence in Court….

Thursday 21st February 2019

Email :**to** Jordi Sanchez (ANC - Catalan National Assembly) 28/09/17 to block streets with cars

State Prosecutor: Received!

Sanchez: First time seeing it is in the court– no evidence that opened/read. Court order to read his emails but no expert called to prove opened/read by Sanchez. Sender of email not called as witness.

22

VII.

Contradictory opinion of computer security experts: **Central Section of Information Technology Crimes** (Sección Central de Delitos en Tecnologias de la Información -SCDTI)

Complaints of Investigators:

Whatsapp – not susceptible to live intervention. End-to-end encryption Methods and data extraction and decryption tools to recover essential data.

Twitter – Who is behind various profiles - personal data used to create, IP, ….

Emails – Intervened by Civil Guard - **no technical analysis as to when/if read by recipient.**

Auto destructive SMS

23

TRIBUNAL SUPREMO
Causa especial 20907/2017

4 month trial
8 months later the Judgment for failed attempt to split from Spain

493 pages

24

9 Catalan independence leaders prison sentences between 9-13 years

Oriol Junqueras: Former VP of Catalonia & leader of Catalan Republican Party (ERC) **13 years**

Jordi Sànchez: **Activist** Ex-President of the civil association ANC **9 years**

Jordi Cuixart: Activist President of civil association Òmnium Cultural **9 years**

Raül Romeva: Former Catalan Minister of Foreign Affairs **12 years**

Jordi Turull: Former Catalan Minister of State **12 years**

Josep Rull: Former Territorial Minister **10 years**

Joaquim Forn: Former Catalan Interior Minister **10years**

Dolors Bassa: Ex social welfare Minister **12 years**

Carme Forcadell: Ex-speaker of the Catalan Parliament **11.5 years**

Former Head of Catalan Regional Government **Carles Puigdemont** fled Spain in the wake of the unilateral declaration of independence. Has been living in Belgium ever since.

22 June 2021 Spain pardons the leaders

23 Sept. 2021 Puigdemont arrested in Italy

25

Judgement No. 5
Provincial Audience (Audiencia Provincial) Madrid, Sección 17ª, Sentencia 132/2020 de 2 Mar. 2020, Rec. 536/2019

Islam. Public profile. Convicted 2.5 years. 540 friends sufficient

26

Judgement No.6
Provincial Audience (Audiencia Provincial) Valencia, Section 2ª, Judgment 468/2020
19 Nov. 2020, Rec. 44/2020

Glorifying terrorism and incitement to hatred

No followers no consequences.

No real or imminent danger

27

28

64 YouTube

Juagement No. 7
Supreme Court(Tribunal Supremo) Sala Segunda, de lo Penal, Sentencia 135/2020 de 7 May. 2020, Rec. 3344/2018

Pablo Hasél
1st Rapper imprisoned in Europe

29

64 YouTube

Pablo Hasél

Glorifying terrorism & libels and insults to the Crown and Police

64 tweets (2014-16) including references to banned guerilla groups, comparing a court to Nazis, calling former monarch Juan Carlos I a mafia boss.

30

64

Pablo Hasél

Glorifying terrorism & libels and insults to the Crown & Police

Controversial lyrics in YouTube

Imprisoned from 15/02/2021

11/03/2021 Council of Europe Commissioner for Human Rights letter to Minister of Justice of Spain

31

32

33

34

35


Mobile evidence

Judgement No. 8

Criminal Court (Juzgado Penal) number 25
Barcelona, 6 October 2020

Tamara Carrasco

From glorification of terrorism to Public Disorder

Member of CUP (Pro- Independence protestors)

Group for the Defence of Catalan Referendum (GDRC) **Before Referendum**

Committees in Defence of the Catalan Referendum (CDR) **After Referendum of 1/10/17**

36

Tamara Carrasco

Crime: 25/02/18
Text & Audio message in Whatsapp in Group about Tsunami of Protests – road blocks on major highways and acts of sabotage (5) related to detention & imprisonment of Catalan Independence leaders and the detention of Former Head of Catalan Regional Government Puigdemont in Germany

All actions subsequently occurred.

37

Tamara Carrasco

+ was in various videos (25/11/2017) in Twitter as member of CDR
-identified by local police (Mozos) in motorway which had been blocked on the same day (27/03/2018)
Analysis of mobile and hardware – partially recuperated evidence. Possible deletion of Whatsapp. Timing of deletion coincided with timing of distribution of the audio message. Acquitted. Source of Whatsapp not investigated. Whatsapp did not incite public disorder. No proof of distribution beyond Whatsapp group. Talk of max. numbers in a group. September 2021 appeal

38

Whatsapp & sister-in-law

Judgment No. 9
Supreme Court
Case No. 599/2021, 7th July, 2021

Crime: Harrassment. Otilia and her Sister-in-Law, Montserrat

Otilia 500 whatsapps, various SMS & stalking Montserrat

Convicted.1 year.

39

Innovative tools for Digital Investigation

Blackbag Technologies

BlueBear

Magnet Forensics

Cellebrite

AccessData

Sumuri Forensics Simplified

Oxygen Forensics

MSAB

Lleida. Net

40

Thank you

Images:

The Noun Project,: Megan Chawn, Adrien Coquet, Monkik, Sebastian Wiercinkski, Skip The Line Barcelona

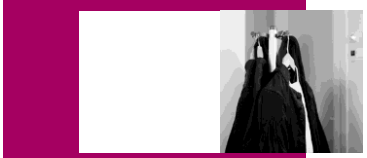
https://www.freepik.com/vectors/logo" >Logo vector created by myriammira - www.freepik.com

https://www.freepik.com/premium-photo/compliance-rule-law-regulation-graphic-interface-business-quality-policy_9003591.htm#query=law%20and%20technology&position=12

https://www.freepik.com/free-vector/protest-demonstration-people-isometric-icons-
Background photo created by rawpixel.com - www.freepik.com
set_4270093.htm#page=1&query=activist%20icon&position=12

41

42



Too Hot to Handle?

Electronic Evidence in Court

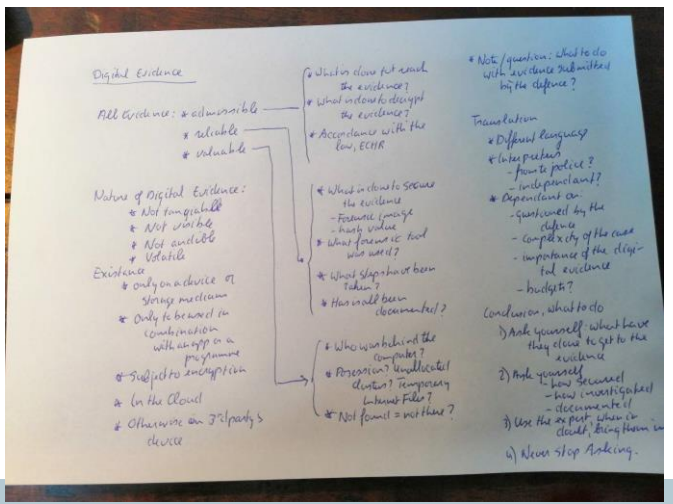
Co-funded by the Justice Programme of the European Union 2014-2020

ERA

de Rechtspraak
Gerechtshof
's-Hertogenbosch

1

The Map



Prague, October 18 & 19, 2021

de Rechtspraak
Gerechtshof
's-Hertogenbosch

2

3 Aspects to Evidence

Key to all evidence:

- Is it admissible?
- Is it reliable?
- Is it valuable?

Look and Feel of Electronic Evidence

- Not Tangible
- Not Visible
- Not Audible
- Volatile

Existence

- Only on a device or storage medium
- Only useful in combination with an app or other piece of software
- Subject to easy or default encryption
- Might be stored in the cloud
- Or otherwise on 3rd party device

Admissibility

- What did the police do to reach the evidence?
- What did they do to decrypt the evidence?
- Were these actions in accordance with the law, the ECHR
- Was he breach of privacy necessary?
- Was it apropriate in relation to the seriousness of the crime?

Examples

- Searching in a smartphone*
- Extortion or illegal promises to obtain passwords
- Forced use of biometrics
- Running a Darkweb marketplace*
- Cross border examinations*

Reliability

- What did the police do to secure the evidence? Forensic Image? Hashvalue?
- What Forensic Tool was used?
- What steps have been taken?
- Has it all been documented?

Value

- Who was operating the divice?
- Posession means control. Unallocated clusters? Temporary Internetfiles?
- Not found = not there?

Note/Question

- What to do with electronic evidence submitted by the defence?
- What to do with evidence you find yourself in open sources?

When in Court

Presentation:

- Witness or expert statements
- Police reports of expert reports
- Screenshots
- Sound recordings
- Printouts

There is no such thing as the original!

Translation

- Lawyers use words
- Data uses bits and bytes
- “Translation” by experts
- Experts in computer forensics may be employed by the police or by independant organisations (or be self-employed)

Independent Experts

Do not rely on police expertise only

- When the evidence is questioned by the defence (with reasonable arguments)
- In complex cases with many electronic aspects
- When electronic evidence is very important or decisive
- If you can rely on a budget…..

Conclusion/What to do?

1. Ask yourself: What was done to get this evidence?
2. Ask yourself: How was it secured, investigated and was that documented?
3. Questions unanswered or when in doubt: bring in the expert.
4. Never Stop Asking!

Internet and Social Networks

- Publicly known facts need no further evidence
- What could be found easily on the web could be such a fact
- Depending on the reliability of the internetsource and what query was needed to find the information
- When in doubt, mention the source in court and have it recorded

Internet and Social Networks

- Police may surf Social Networks like any other person
- No further authorisation needed
- No objection to surfing under a fake name

- However:
- When aspects of someone's private life are revealed or recorded a prosecutor's order is needed (or a court order)
- Actively interfering in contacts or groups is also ruled by special legislation

Smartfones

17

18

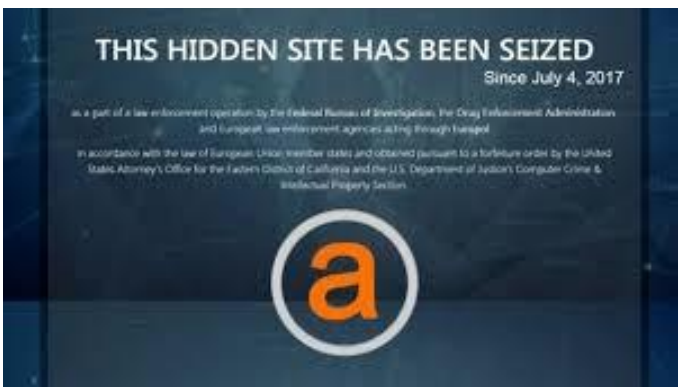
Changing Legal Regime

ECLI:NL:HR:2017:584

Before: If you seize an object, you may search it, including stored data

After: Rule stands, but not if your search means a serious breach of privacy,
If that's the case you need a prosecutor's order
If the search causes a very serious breach you need a court order.

Alpha Bay



Alpha Bay

- Dark Web
- 1 of Big 3, 200.000 users 40.000 vendors
- Since 2014 at least $ 1 billion traded
- Taken down July 4th 2017, why then?

Hansa Market

Hansa Market

- Investigation since 2016 FBI, DEA and NL
- 2 operators in Germany, servers in Germany, NL en Lithuania
- Taken over and operated under NL judicial authoriy on june 20st 2017
- After july 4th, visit boosted 1000 to 8000 daily
- 1000 transactions daily

Hansa Market

- Questions:
- Was the evidence legally obtained?
- Police facilitating illegal transactions?
- How was the evidence stored and processed?
- Cross border evidence?

The Court Decision

ECLI:NL:RBROT:2019:5339

38.709 pillen XTC, en/of
63.742 trips/hoeveelheden LSD, en/of
95.855,35 gram molly/MDMA, en/of
3.912 capsules MDMA, en/of
5.019,2 gram cocaïne, en/of
129 gram meth/amfetamine,

The Court Decision 2

-There is a legal basis: Infiltration
-Thoroughly protocolles
-Clear insight in operation
-No other effective means to put an end to this
-No provocation

Conclusion: prosecution may be recieved, evidence admissible

Ennetcom

Ennetcom

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

Ennetcom

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

Ennetcom

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

Ennetcom

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

Ennetcom

- Questions:
- What steps are taken from seizure?
- Reliability of identification proces
- Exculpatory evidence disappeared?
- No context available, consequence?
- David Graus: “Naive and Unreliable method” Invalid verifiability.

Enchrochat, one step further

- Law enforcement agencies hacked the server of the service provider
- Handheld devices connected to the server and were infected
- Messages intercepted before encryption
- Decryption passwords intercepted

- Tremendous impact in terms of intelligence and investigations
- But what are the legal implications of:

- No full disclosure of the operations
- Cross border hacking
- Goldmine for lawyers

ANoM

- FBI arrests a man who owns and exploits an encrypted network
- Suspect offers cooperation
- FBI sells encrypted handhelds through undercover agents and storefronts
- Subjects talk freely about drugs, guns and money

- Fruitful harvest of intelligence, money, quantities of drugs and arrests
- What to do with the evidence?

Thank you for your attention!

John van Krieken LLM MMO
Court of Appeal ‘s-Hertogenbosch
j.van.krieken@rechtspraak.nl
+31648135890

Prague, October 18 & 19, 2021

de Rechtspraak
Gerechtshof
's-Hertogenbosch

35

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

Handling Electronic Evidence in Courts

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

1

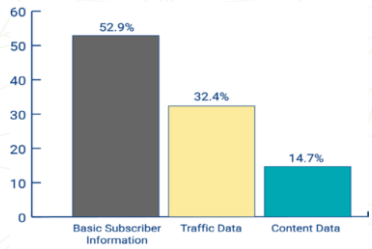
CYBERCRIME AND DIGITAL EVIDENCE

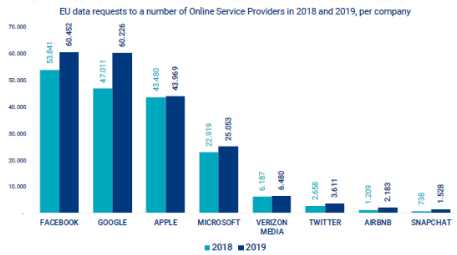
Focus	2018	2019	2020	2018	2019	2020	2018	2019	2020	2018	2019	2020
Migrant smuggling	71	86	99	17	24	21	3	2	2	12	12	12
THB	150	183	163	43	54	56	0	4	2	56	61	48
Terrorism	84	95	69	20	24	12	0	0	0	12	8	7
Cybercrime	98	126	174	28	34	45	2	3	1	10	17	21
Corruption	78	76	93	19	14	8	0	0	0	6	5	5
Drug trafficking	450	463	562	78	80	87	0	2	4	42	51	50
Environmental crime	24	14	20	6	8	6	0	1	0	4	6	6
Money-laundering	436	531	595	94	138	101	6	6	7	49	72	64
Swindling and fraud	909	1112	1264	87	112	91	7	12	8	50	64	68
MOCG	273	312	380	26	20	19	1	2	1	15	17	13
PIF	56	140	128	9	15	20	1	2	2	8	11	10
Core international crimes	n/a	n/a	12	n/a	n/a	2	n/a	n/a	0	n/a	n/a	0

2

CYBERCRIME AND DIGITAL EVIDENCE

- Digital evidence will be needed in around 85% of criminal investigations
- In two-thirds of these investigations, it is necessary to obtain it from OSPs established in another jurisdiction – increasing numbers
- Not clearly regulated and 26 % EU countries not allowed direct request to OSPs





3

EUROPEAN JUDICIAL CYBERCRIME NETWORK

- **WHO WE ARE :**
- Network of Judicial Authorities specialized in cybercrime and digital evidence
- Contact Points in EU Member States plus Norway, Switzerland and Serbia
- Established by the Council Conclusions of 9 June 2016
- Hosted and supported by Eurojust

4

EUROPEAN JUDICIAL CYBERCRIME NETWORK

- **OUR MISSION IN CYBERCRIME AND E-EVIDENCE:**
- Provide access and disseminate information
- Provide a forum for discussions of practical and legal problems
- Exchange information on domestic legislation, relevant case law, international cooperation and best practices
- Promote the use of Eurojust in cross-border cases

5

EUROPEAN JUDICIAL CYBERCRIME NETWORK

- **OUR ACTIVITIES:**
- Two Plenary Meetings per year for expert practitioners
- Develop expertise in Subgroups of Data Retention, Digital Evidence, Virtual Currencies, Training
- Contribute to deliverables of stakeholders and produce our own on encryption, digital evidence, virtual currencies…
- Participate in training activities

6

EUROPEAN JUDICIAL CYBERCRIME NETWORK

- **HOW WE CAN SUPPORT YOU:**
- Be a Forum where you can discuss questions with colleagues
- Put you in contact with a colleague from the jurisdiction you need to work with
- Help you give your case an international perspective for possible extension to other jurisdictions
- Share the knowledge of relevant products for your case

7

EUROPEAN JUDICIAL CYBERCRIME NETWORK

The international case perspective – Are you alone ?
Probably not…
Criminals did not act alone neither should you

RANSOMWARE
CYBERVIOLENCE
ONLINE INVESTMENT FRAUD
BOTNETs
VIRTUAL CURRENCY MONEY LAUNDERING

8

Challenges in Cybercrime Investigations

CYBERCRIME – DIGITAL EVIDENCE		
LEGAL	**BOTH**	**TECHNICAL**
Data retention regimes	Encryption	Transfer of data
Admissibility	Chain of Custody	Seizure of large amounts of data
Jurisdiction	Seizure of Virtual Currencies	
	Victim Remediation	
	Rights of 3rd parties	

Challenges in Cybercrime Investigations

New technology - Old laws

How to apply old laws made under the concept of physical objects to digital objects ?

Fast paced evolution of Tech – need for training and constant updates

The Future?

New roles and mind-set on how to present digital evidence and analyse its admissibility

Challenges to Cybercrime Investigations

- **CASE EXAMPLE – Domestic Violence**

The victim is threated, bikini pictures and full contacts of her for sexual encounters are shared in a fake Facebook profile.

Police tracks the IP Address of one of the messages to an address shared by the suspect and his grandmother. Suspect denies facts. Times of the messages and posts coincide with the time suspect alleges to be playing football with a brother.

Brother confirms his version.

11

Challenges in Cybercrime Investigations

- **CASE EXAMPLE – Corruption**

A MP is investigated for corruption, as a suspect of receiving an apartment to get approval for a legislation benefiting company X.

In a search to his personal computer, e-mails and documents stored in the “cloud” were seized. They portrait conversations with an executive of X about the apartment and 3D models to decorate it.

On trial, the MP denies being the owner of the apartment and claims Police manipulated the e-mails.

12

Challenges in Cybercrime Investigations

- COOPERATION WITH OSPs
- DATA RETENTION
- UNDERSTANDING E-EVIDENCE – TRAINING
- LOSS OF LOCATION
- DIRECT CROSS BORDER ACCESS TO DIGITAL EVIDENCE
- EXTENDED SEARCHES
- CHAIN OF CUSTODY

13

DIGITAL EVIDENCE

STORED E-EVIDENCE	
BASIC SUBSCRIBER INFORMATION - BSI	Information on the identity of the subscriber/user, address, IP address of the first login, billing and payment information, any other information on the site of the installation of communication equipment, how long the service has been used. Art. 18. n. 3 Budapest Convention
TRAFFIC DATA – NON CONTENT DATA	Any computer data relating to a communication indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service – ex. IP or MAC addresses (metadata), access logs, transaction logs. Art. 1. al. d) Budapest Convention
CONTENT DATA	Body or text contained in the communication, such as an e-mail, post, image, video...
REAL TIME GATHERING OF E-EVIDENCE	
TRAFFIC DATA	Interception of who the suspect is contacting and where from – ex. with reference to IP addresses. Art. 20. Budapest Convention
CONTENT DATA	Interception of the body or text contained in the communication, e-mail text, post, image, video... Art. 21. Budapest Convention

14

DIGITAL EVIDENCE

TRUE complete **RELIABLE** credible

PROPORCIONATE

Investigation vs. fundamental rights of the suspect

Supported by a **STANDARTZIED** forensic report

15

DIGITAL EVIDENCE SEARCH AND SEIZURE

- **Traditional search** tangible form
- LEA search the location, inspect and seize documents or objects during procedure

HOW IS THIS DIFERENT WITH E-EVIDENCE ?

- Intangible form
- May be stored in a different location of the device but readily accessible to that system.

16

DIGITAL EVIDENCE

- **Stored on the suspect's device in our jurisdiction**
- Seizure and forensic analysis accordingly to national law
- **Stored on server property of third-party abroad or unknown location**

OSINT, MLA, EIO, voluntary cooperation of SPs in their legal framework and their own compliance rules

CHAIN OF CUSTODY – FUNDAMENTAL RIGHTS

17

The Future ? Blockchain ?

Blockchain technology could provide a platform for chain of custody assurance along the investigation and trial, in a trustworthy easy to consult format.

18

MAIDAN SQUARE MASSACRE CASE

The 2014 EUROMAIDAN took the life of more than 100 people in Ukraine.
More than 100 protesters were allegedly shot by police and snipers loyal to the Government.

19

MAIDAN SQUARE MASSACRE CASE

- 3 D Modelling of events to analyse conflicting narratives
- 65 hours of video, surveys, autopsy reports
- Spatial (3D) and temporal (4D) reconstruction of the event
- Interactive presentation platform with evidence, analysis, reconstruction animations and an archive of geolocated and synchronized source videos

20

EUROPEAN JUDICIAL CYBERCRIME NETWORK

- **Resources:**
- **European Judicial Cybercrime Network**

https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network

- **Digital Evidence Situation Report**

https://www.eurojust.europa.eu/sirius-eu-digital-evidence-situation--report

- **Guide on Article 6 of the European Convention on Human Rights**

https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf

- **Locard Project**

https://locard.eu/faqs

- **Euromaidan 3D Reconstruction**

https://www.cmu.edu/chrs/cases/euromaidan.html

21

EUROPEAN JUDICIAL CYBERCRIME NETWORK

More than half of all criminal investigations today include a request for access to e-evidence such as texts, emails or messaging apps. In response to the growing need for transnational access to digital evidence, Europol, in close collaboration with Eurojust, created the SIRIUS Project in October 2017. The project is a platform that helps **judicial authorities** address complexity and volume of information online, providing guidance, tools and exchange of peer experiences.

REGISTER

SCAN ME

https://ec.europa.eu/eusurvey/runner/Sirius
Password : SIRIUS
For more information contact sirius.eurojust@eurojust.europa.eu

22

Cláudia Pina

SNE for Casework Unit – Coordinator of EJCN Support Team

CPina@eurojust.europa.eu

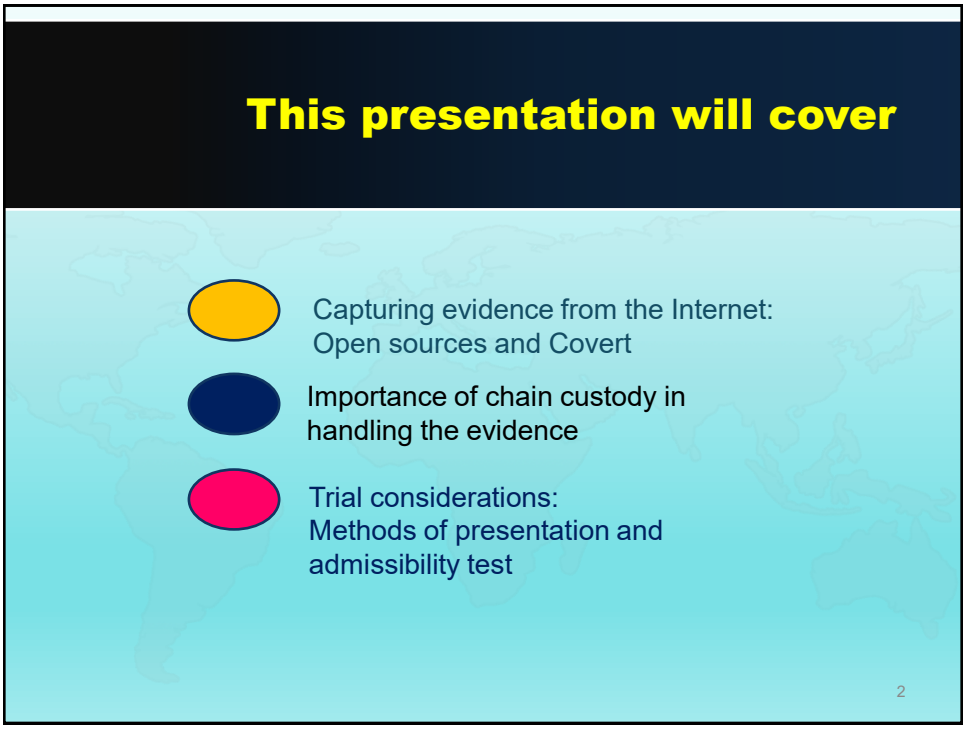
+31 70 412 5572

www.eurojust.europa.eu

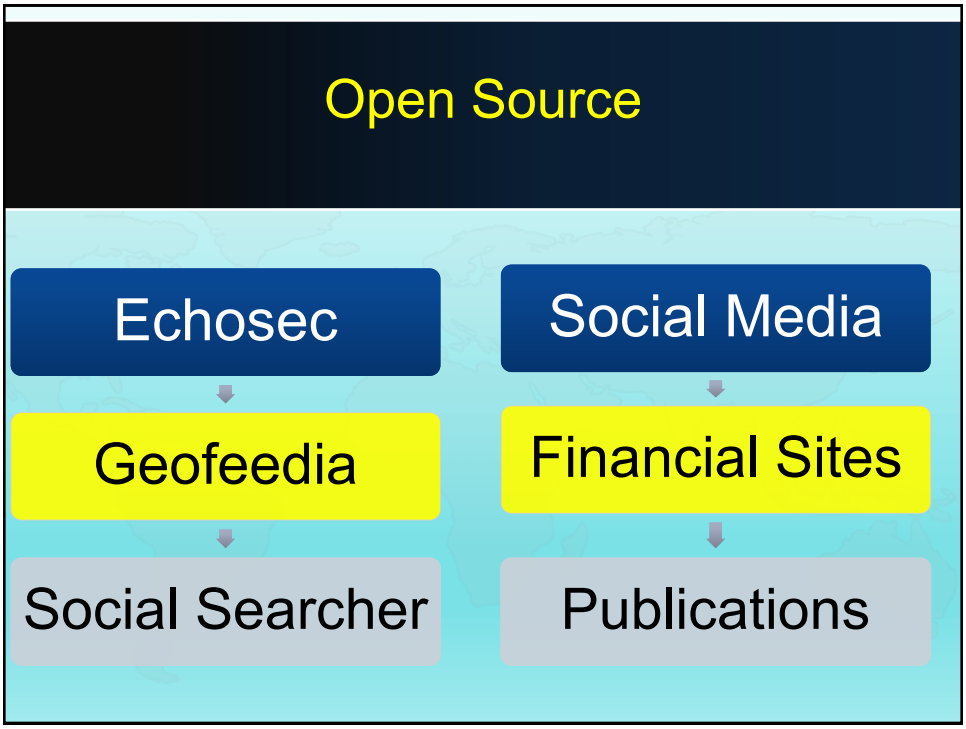
Follow Eurojust on Twitter and LinkedIn @ *Eurojust*


Online Investigations and the Challenges for the Defence
Co-funded by the Justice Programme of the European Union 2014-2020
Aliant Law
Muthupandi Ganesan
Barrister-at-Law
19 October 2021, Prague

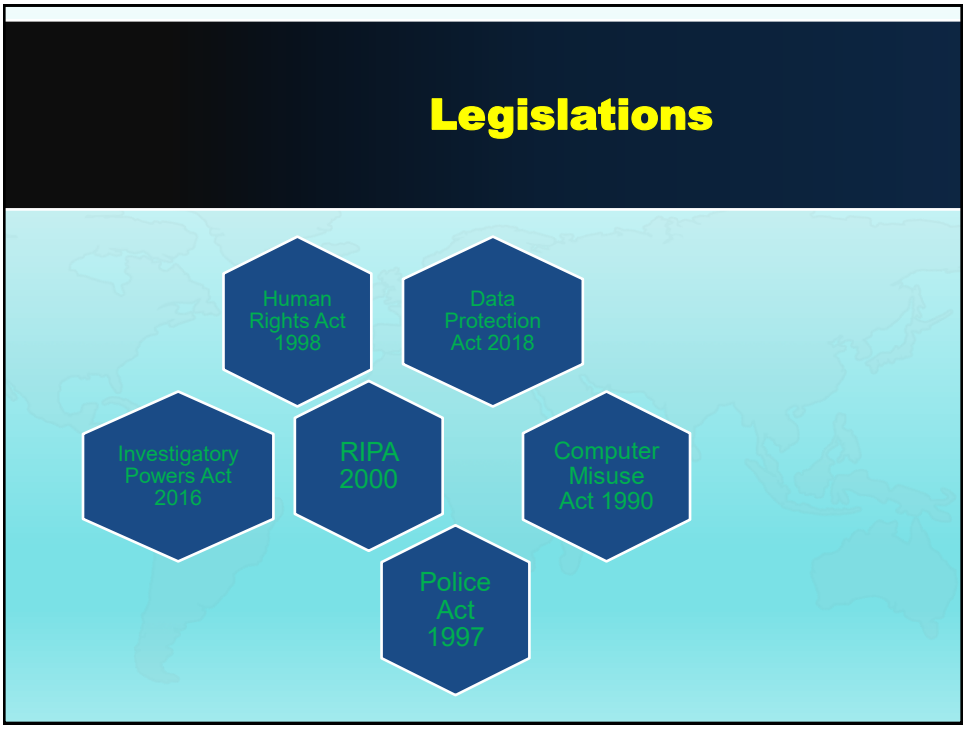
1


This presentation will cover
Capturing evidence from the Internet: Open sources and Covert
Importance of chain custody in handling the evidence
Trial considerations: Methods of presentation and admissibility test
2

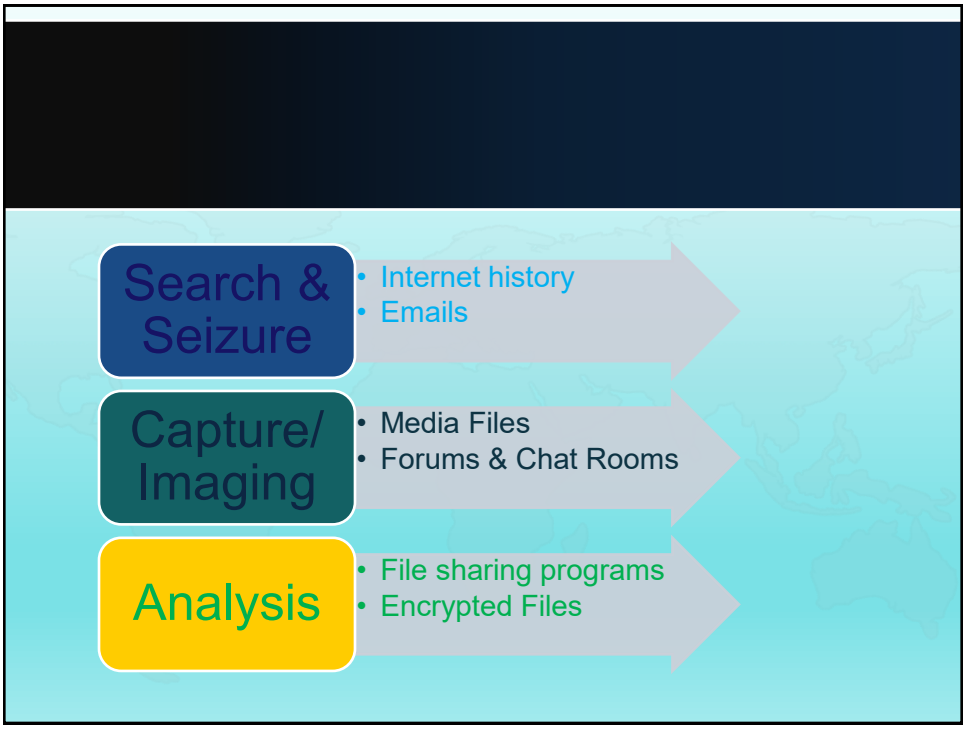
2


Open Source
Echosec
Geofeedia
Social Searcher
Social Media
Financial Sites
Publications

3


Legislations
Human Rights Act 1998
Data Protection Act 2018
Investigatory Powers Act 2016
RIPA 2000
Computer Misuse Act 1990
Police Act 1997

4


Search & Seizure
Internet history
Emails
Capture/ Imaging
Media Files
Forums & Chat Rooms
Analysis
File sharing programs
Encrypted Files

5


Witness Statements
Reports
Expert Evidence

6

NPCC Guidance on Open Source Investigation / Research

ACPO – Good Practice Guide for Digital Evidence – March 2012

ACPO - Good practice Guide for Computer-Based Electronic Evidence (v4.0)

7

General principles

The general principles to be followed by investigators in handling and examining digital material are:

(i) No action taken by investigators or their agents should change data held on a computer or storage media which may subsequently be relied upon in court;

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

(iii) An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes; and,

(iv) d. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are followed.

(Attorney General's Guidelines on Disclosure: For investigators, prosecutors and defence practitioners – December 2013 but updated March 2018)

8

Digital evidence – International Issues

59.The obligations under the CPIA Code to pursue all reasonable lines of enquiry apply to material held overseas.

60.Where it appears that there is relevant material, the Prosecutor must take reasonable steps to obtain it, either informally or making use of the powers contained in the Crime (International Co-operation) Act 2003 and any EU and International Conventions. See CPS Guidance 'Obtaining Evidence and Information from Abroad'.

9

Types of guidance

- CPS Guidance 'Obtaining Evidence and Information from Abroad
- Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice
- Mutual Legal Assistance
- Extradition

10

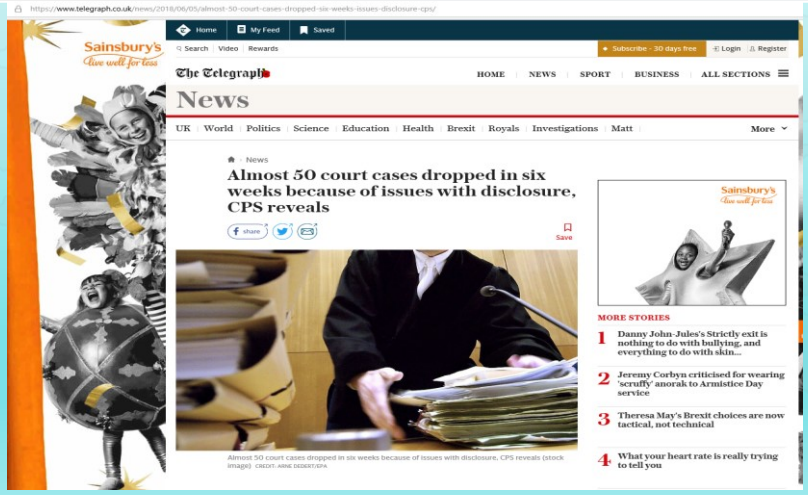
Disclosure – Practical Issues

- Volume of Data
- Funding
- Equipment
- TRAINING:

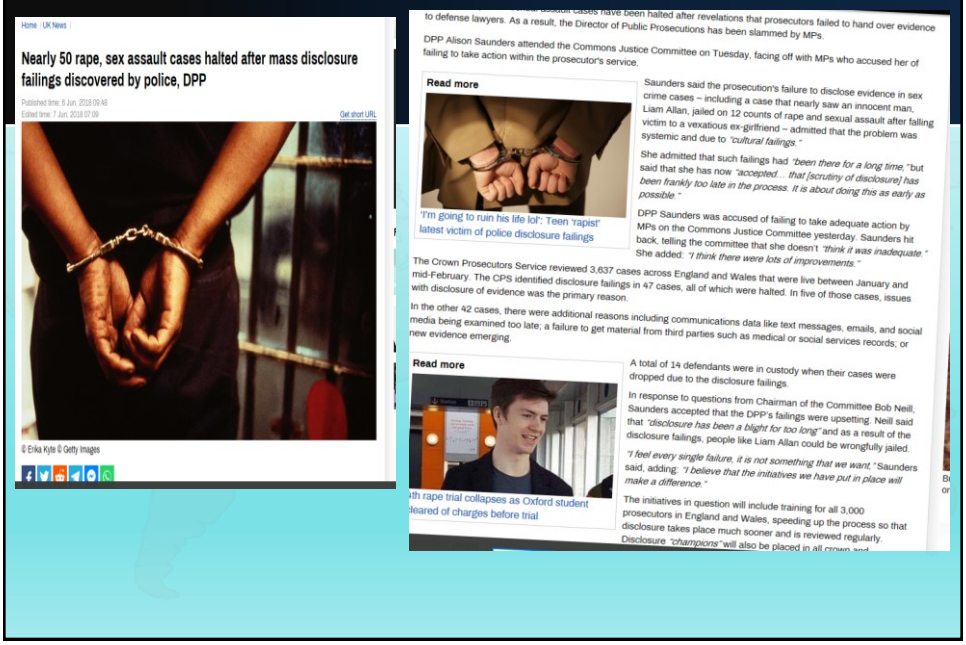
  For Judges, Prosecutors, Defence Lawyers and Clients
- NATURE OF EVIDNECES:

  CCTV, Text messages, Social Networking, Exchange of Data, WhatsApp messages

11



12



13

DISCLOSURE: QUALITY OF KNOWLEDGE : JUDGE VERSUS JURY

- Security & Authenticity of Data
- Accuracy
- Continuity
- Telephone Data / Telephone Master Data
- Presentation of Data to the Jury

14

EXPERT EVIDENCE IN DIGITAL / CLOUD COMPUTING

It should always be kept in mind that expert evidence is merely one tool to be used in proving a case. The danger in placing too much reliance on the findings of experts is demonstrated in a series of cases in relation to DNA analysis, where there was no other evidence against the accused save the presence of his DNA found at the scene of a crime. The Court of Appeal has emphasized that expert evidence can only be judged in the light of the other evidence in the case. In these cases, the absence of any other evidence, however limited, should have been fatal to the case being charged - see R v Doheny & Adams (1997) 1 Cr. App. R. 269 (at paragraph 372).

The dangers of an over-reliance on expert evidence without considering the significance of the other evidence in the case is a factor that prosecutors need to consider in reviewing any file presented by the police for advice and review.

15

Expert Witness

Section 30 of the Criminal Justice Act 1988 & Criminal Procedure Rules – Part 33

1. Assistance to the Court
2. Relevant Expertise
3. Impartial
4. Evidence is reliable

Definition of Expert Witness: An expert witness is a witness who provides to the court a statement of opinion on any admissible matter calling for expertise by the witness and is qualified to give such an opinion.

The Duty of an Expert Witness: The duty of an expert witness is to provide independent assistance to the court by way of objective, unbiased opinion in relation to matters within their expertise. This is a duty that is owed to the court and overrides any obligation to the party from whom the expert is receiving instructions - see R v Harris and others [2005] EWCA Crim.1980.

16

Expert evidence: Challenges

1. By an application to the judge (on a voir dire or at a case management hearing) to exclude expert evidence that is biased, unhelpful or unreliable evidence under section 78 PACE and R v Turner (1975) 60 Cr. App R. 80;
2. By an application to the judge to exclude expert evidence due to noncompliance with Criminal Procedure Rules;
3. By requesting that evidence be edited to remove comment on matters outside of expert's experience, or amended where conclusions are overstated;
4. By requesting the preparation of a joint expert's report may result in reports being amended to more accurately reflect the underlying science; or •
5. By testing the expert's hypothesis in cross examination to ensure it has been the subject of sufficient scrutiny and peer reviews. For example, in drink driving cases, where defence experts produce new and unproven claims about breath test machines suffering from "long blow" or "long purge". There is no accepted legal basis for either claim.

17

Expert evidence: expertise must be reviewed carefully!

18

Cybercrime Legislation

Functions of cybercrime legislation

- **Setting clear standards of behaviour for the use of computer devices**
- **Deterring perpetrators and protecting citizens**
- **Enabling law enforcement investigations while protecting individual privacy**
- **Providing fair and effective criminal justice procedures**
- **Requiring minimum protection standards in areas such as data handling and retention**
- **Enabling cooperation between countries in criminal matters involving cybercrime and electronic evidence**

19

Cyber crime legislation

1989	• Council of Europe - 'Expert Report on Computer-Related Crime
2001	• Council of Europe Convention on Cybercrime
2011	• Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography
2013	• Directive 2013/40/EU on attacks against information systems.

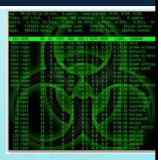
20

Cyber crime legislation: Problems

- Basic / Universal Standards
- Protection v Rights
- Law Enforcement & Jurisdiction
- International Co-operation

21

Complexity



- International Treaties / Obligations
  - Practical Problems
    - Capacity & Training
    - Attribution & detection
  - Legal Problems
    - Lack of mutual legislation & treatment
    - Lack of co-operation

22

Questions?

Muthupandi Ganesan
Barrister-at-Law
Aliant Law

23

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

NSZ ČR

E-Evidence Gathering in Czech Republic Theory and Practise

Pavel Zeman

General Prosecutor´s Office

NSZ ČR

E-Evidence

- Rapid development of electronic communications and technologies
- Legislation remains more or less the same as it was in times of no cybercrime
- “We are combating cybercrime in 21st century with weapons of 20th century“
- We try to apply procedural rules designed for collection of evidence in real world to e-evidence from virtual world
- Huge requirements for interpretation and application skills of law enforcement and justice
- Space of manoeuvre for defend lawyers
- Very often contradictory court decisions

NSZ ČR

Term of E-Evidence in General Art. 89 CPC

- Evidence may be anything that can help to clarify the case, in particular testimonies of the accused and witnesses, expert opinions, items and documents relevant to the criminal proceedings, and examinations. Each party may find, present, or propose to produce evidence. The fact that the law enforcement authority did not find or request a piece of evidence is not grounds for rejecting such evidence.
- Evidence obtained by unlawful coercion or by threat of coercion may not be used in the proceedings except when used as evidence against the person that used coercion or threatened with coercion.

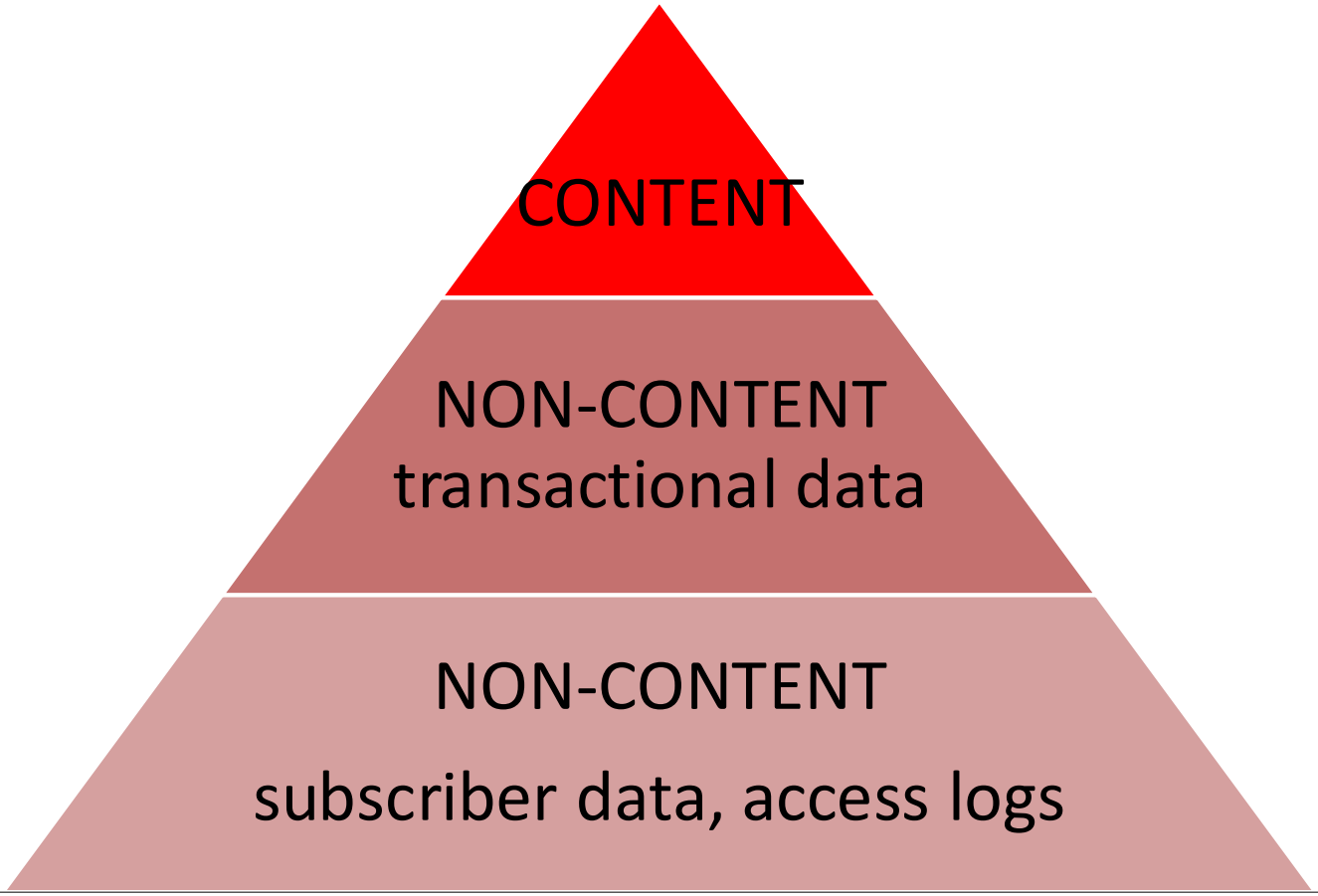
NSZ ČR

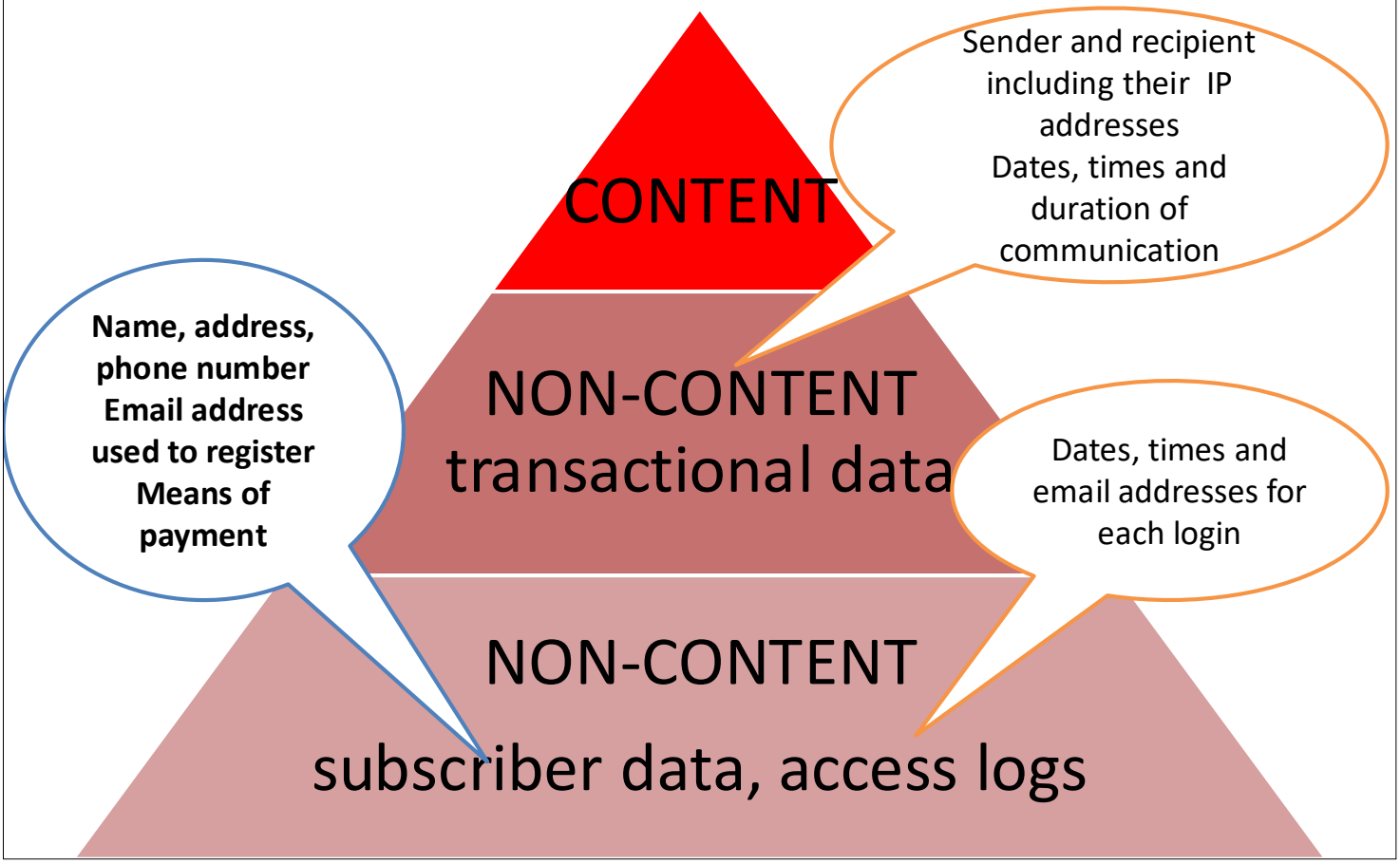
E-Evidence

- Evidence definition in penal proceedings is rather simple
- Its application limitation is minimal-just for evidence obtained illicitly
- Defence tries to limit usage of individual evidence (or even to refuse its admission)-this issues are being handled in every bigger case
- In the past
  - Accused person usually said that he/she had been illicitly compulsed to confession
- Nowadays
  - Crimes are more sofisticated thus police investigation must be more sofisticated and thus defence is more sofisticated trying to prove the illicit acquisition of evidence, especially e-evidence

E-Evidence

- Very simply said: e-evidence is DATA
  - Thus DATA is an immaterial thing (for the purposes of this presentation)
- DATA in criminal proceedings is a source of certain information
- DATA originates in connection with the use of electronic devices, especially communication devices and they have different form
- For evidence purposes we often use e-evidence originated from human activity (documents, photos, videos, text messages)=DOCUMENTS
- METADATA
  - Side product of DOCUMENT creation
  - Its creation is automatic
  - More and more used as e-evidence





NSZ ČR

Saved Content Data

- Big problem in CZ
- CZ does not have legislation for remote access to computer or for remote computer search
- We thus apply legislation which is primarily written for the surveillance of persons in real world (also here we need the court order)
  - With the help of remote access we usually receive data from email boxes
  - Not used for access to „clouds“ as we have doubts about its legality for this purpose
- Solution - New Penal Procedure

NSZ ČR

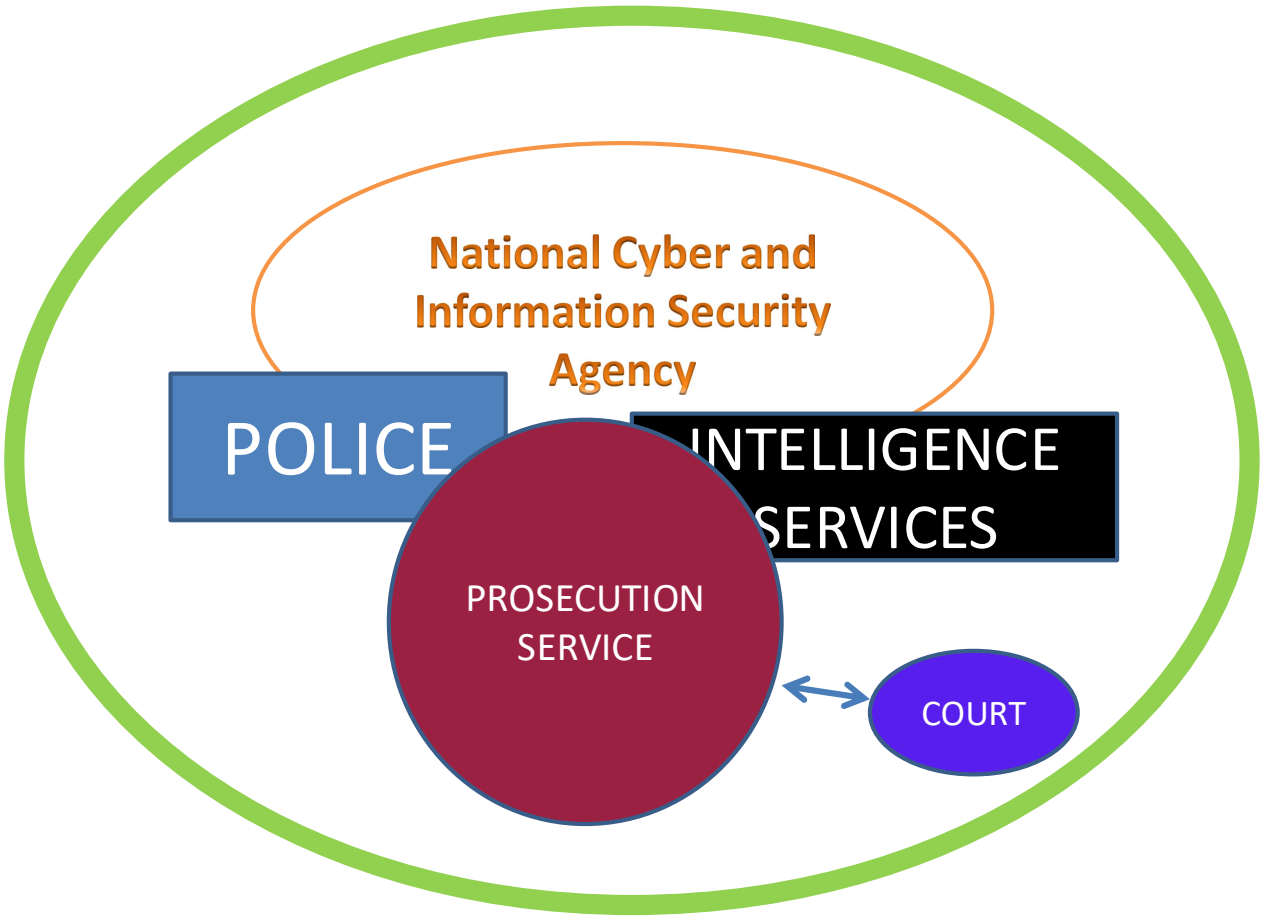
National Cyber and Information Security Agency

POLICE

INTELLIGENCE SERVICES

PROSECUTION SERVICE

NSZ ČR



NSZ ČR

Cooperation
Basic Elements

- TRUST
- WILLINGNESS TO COOPERATE
- COMMUNICATION
  - Signal communication platform
  - Regular meetings of case staff (formal and informal coffee break discussions ☺)
  - Regular meetings of chiefs
- SHARING OF INFORMATION
  - Well-timed alert of problems/cases (Signal platform)
- STRIVE FOR SOLUTIONS RATHER THAN TO SEARCH FOR OBSTACLES
- IMPROVISATION - every time legal

NSZ ČR

Use of E-Evidence Obtained from Other Institutions

- NCISA
  - Law enforcement authorities and judiciary are allowed to use e-evidence secured by NCISA
- Intelligence Services
  - Reminiscence from the past – fear of misuse of intelligence services and their powers and information
  - Thus information from intelligence services must not be transferred as evidence
  - No possibility to obtain e-evidence from intelligence services!!!
  - Only provision of information
  - Various approaches in different countries

NSZ ČR

Attribution

Attribution in cyberspace is the process of determining the perpetrator of a cyber attack which is a foreign state or behind which a foreign state stands.

This process has several levels:

1. Attack identification and information of other participants in the process
2. Securing and collecting evidence of an attack and performing analysis
3. Comparison of evidence and information found by all stakeholders and then identification of the perpetrator (attacking state)
4. Transmission of information to state authorities (politicians) entitled to decide on the use of information
5. Reaction

NSZ ČR

Case "The Hospital of Brno" Example of Bad Practise

- The case of ransomware attack the Hospital of Brno
- Qualified as blackmail (Art. 175 CC) and some other crimes
- The unknown perpetrator carried out a large ransomware attack on the computer system of a large university hospital in Brno
- This attack caused great damage
  - The entire information system of the hospital was paralyzed
  - Many patients had to be transferred to other hospitals
  - No one died just because of the care of the doctors and paramedics
  - More or less hospital returned 30 years back

NSZ ČR

Case “The Hospital of Brno“ Example of Bad Practise

- The investigation shows that the attack was led by malware which was also used in other attacks in other countries in Europe
- At the beginning of the investigation (after the attack was detected), there was an incredible situation
- The Police President learned of the attack from the Interior Minister who heard the information on TV news
- The Head of the Police Cyber Unit learned of the situation from the Police President
- NCISA was already on the scene dealing with the hospital's IT department but no one informed the Police
- Before the Police arrived on the crime scene, the electronic evidence was almost destroyed

NSZ ČR

Case “The Hospital of Brno“ Example of Bad Practise

- Only after the public prosecutor arrived on the crime scene, it was possible to coordinate the activities of the Police, NCISA and IT specialists from the hospital, prevent further damage and at the same time secure necessary electronic evidence
- This case is, regarding communication among stakeholders, one of the worst that has ever happened
- After this experience, all stakeholders have understood that cooperation is necessary

NSZ ČR

III. The "LOCAL" Case

- The crime of an unauthorised access to a computer system (Art. 230 CC)
- At the beginning of 2020, an unknown perpetrator hacked the system of the Ministry of Regional Development for evaluating and monitoring the management of subsidies from European funds
- This system is part of a critical information infrastructure under the Cyber Security Act
- The incident was reported to the Police by the NCISA unofficially but very quickly
- The Police immediately contacted the Ministry of Regional Development as a victim and data from the compromised system was secured

NSZ ČR

III. The "LOCAL" Case

- There are currently two investigative versions:

  a) The perpetrator installed malware to use computers to extract the "Monero" cryptocurrency

  b) At the same time the perpetrator gained access to install malware to control software (Backdoor Notrobin)
- Further requests for data preservation were sent abroad and managed
- NCISA informed the Police and also performed an overall analysis of the hacked system for the Police
- Police is now waiting for the results of MLA requests from US and the Russian Federation, but all steps to identify the perpetrator have been taken in the Czech Republic

Thank you for your attention