OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

SPECIAL INVESTIGATION TECHNIQUES ON MOBILE DEVICES

Thessaloniki, 16-17 February 2023

EXCELLENCE IN EUROPEAN LAW

Speakers

Steven David Brown, International Cybercrime Consultant, Vienna

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

Timothy De Groot, Police Officer, Brussels

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

Sapfo Katsanaki, Prosecutor, Seconded National Expert (SNE), EPPO, Luxembourg

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

Eleni Papadopoulou, Head, Prosecutor's Office, Korinthos

Michael Rothärmel, Head of Unit, Fight against Terrorism and Extremism, Ministry of Justice, Munich

Lampros Tsogkas, Vice Prosecutor, Prosecutor's Office, Court of Appeal, Larissa

Bilal Sen, Senior Investigator, Coninsec, Cologne

Key topics

- Technical issues (internet caches, proxy servers, encryption, deep/dark web, etc.)
- Legal implications of e-evidence (collection, evaluation and admissibility)
- The rise of evidence on mobile devices
- Insights into different national criminal justice systems

Language
English

Event number
322DT58

Organisers
ERA (Laviero Buono) in cooperation with the Hellenic School of Judges

ΕΣΔΙ
NATIONAL SCHOOL OF THE JUDICIARY

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

european.law

Thursday, 16 February 2023

09:00 Arrival and registration of participants

09:30 **Welcome and introduction to the programme**
Lampros Tsogkas & Laviero Buono

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

Chair: Laviero Buono

09:35 **Internet searches and computer forensics in criminal cases: using open-source intelligence to gather evidence online**
- World Wide Web (WWW) vs. the Internet
- Understanding Internet protocols (http, https, ftp)
- Internet cache – deleting and retrieving
- Surface search vs deep web search
- Meta search engines
- Proxy servers

Steven David Brown

10:45 Discussion

11:00 Break

Chair: Laviero Buono

11:30 **Digital evidence collection: Open Source Intelligence (OSINT)**
- Introduction and the role of OSINT
- Efficient dialogue with searching engines
- Use case scenarios and OSINT tools
- Live case demonstration

Bilal Sen

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

13:45 **Handling electronic evidence on mobile devices in court: experiences in Greece**
Sapfo Katsanaki

14:30 **Cross-border interception measures: legal challenges and solutions**
- Cooperation tools
- Direct cross-border interception without technical assistance
- Admissibility of evidence
- Data retention

Michael Rothärmel

15:15 Discussion

15:30 Break

Chair: Federico Donelli

16:00 **The proposed European Production Order (EPO) and its effectiveness in collecting evidence (including evidence stored on mobile devices)**
- Legal framework and problems regarding traditional MLA in the digital age
- The EPO in the online context

Objective

Mobile devices such as smartphones and tablets contain personal information including call history, text messages, e-mails, digital photographs, videos, calendar items, address books, passwords and credit card numbers. They can be useful as sources of digital evidence to be examined when criminal activities occur.

This seminar aims to share advanced knowledge and to exchange experience and best practice between judges, prosecutors and lawyers in private practice who deal with criminal proceedings involving e-evidence on mobile devices.

About the Project

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

Who should attend?

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

Venue

National School of Judges
Ikaron str, PC 55102
Kalamaria, Thessaloniki
Greece

CPD

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

- Specificities and challenges of criminal cases where anonymous networks and encrypted files are involved

Jordy Mullers

16:45 Discussion

17:00 End of first day

20:00 Dinner offered by the organisers

Friday, 17 February 2023

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

Chair: Jordy Mullers

09:30 **The collection of evidence located abroad and the challenges of transborder access to data**
- Search across jurisdictions / devices seized
- Transborder access to data
- Cloud computing
- European enforcement challenges in the online context
- Shortcomings and remedies

Federico Donelli

10:15 **Where's my phone?**
- Comparing and contrasting cell site analysis with GPS systems for locating a phone
- Geofence warrants
- IMSI (International Mobile Subscriber Identity) catchers: their use and concerns about their deployment

Steven David Brown

11:00 Discussion

11:15 Break

11:45 **Technical insights for the preparation, identification and preservation phase**
- The importance of the chain of custody in handling the evidence
- Case studies

Timothy De Groot

12:15 **E-evidence in child sexual abuse cases**
Eleni Papadopoulou

12:45 Discussion

13:00 End of seminar and lunch

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

Apply online for
"Obtaining e-evidence when investigating and prosecuting crimes":
www.era.int/?131810&en

Your contact persons

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

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

Save the date

Annual Conference on Countering Terrorism in the EU 2022
Online, 8-9 December 2022

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

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

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

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

Application

Obtaining e-evidence when investigating and prosecuting crimes

Thessaloniki, 16-17 February 2023 / Event number: 323DT58/SBa

Terms and conditions of participation

Selection

1. Participation is only open to judges, prosecutors and lawyers in private practice from eligible EU Member States.
2. The number of places available is limited (30 places). Participation will be subject to a selection procedure.
3. Applications should be submitted before **28 January 2023**.
4. A response will be sent to every applicant after this deadline.
   We advise you not to book any travel or hotel before you receive our confirmation.

Registration Fee

5. €225 including documentation, lunches and dinner.

Travel expenses

6. Travel costs up to €300 can be reimbursed by ERA upon receipt of the original receipts, tickets, boarding passes, invoices after the seminar. Participants are asked to book their own travel and accommodation. These rules do not apply to representatives of EU Institutions and Agencies who are supposed to cover their own travel and accommodation. Participants are advised of the obligation to use the most cost-efficient mode of transport available.

Accommodation

7. Maximum 2 hotel nights single use up to €150.00 per night can be reimbursed by ERA, only upon receipt of the original hotel invoice. This is only for participants from more than 100km away 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 online for "Obtaining e-evidence when investigating and prosecuting crimes": www.era.int/?131810&en

Venue

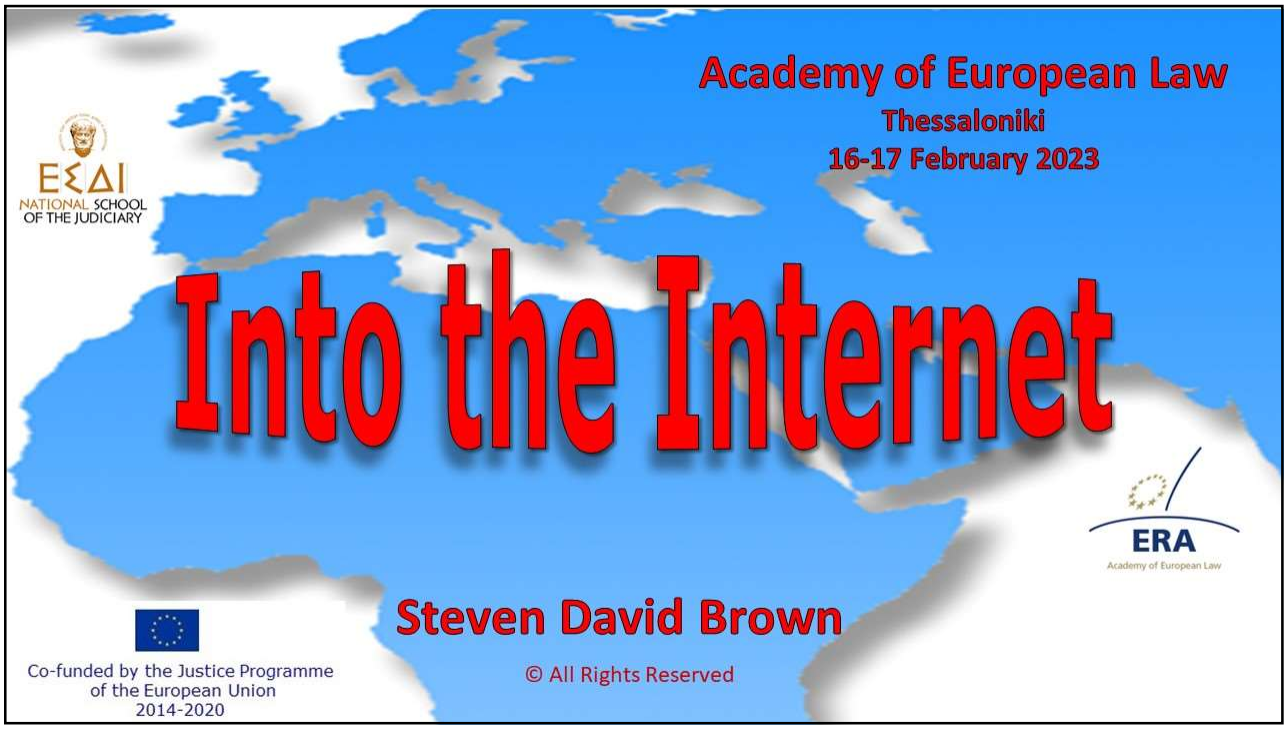
National School of Judges
Ikaron str, PC 55102
Kalamaria, Thessaloniki
Greece

Language

English

Contact Person

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



1

What is the Internet ?

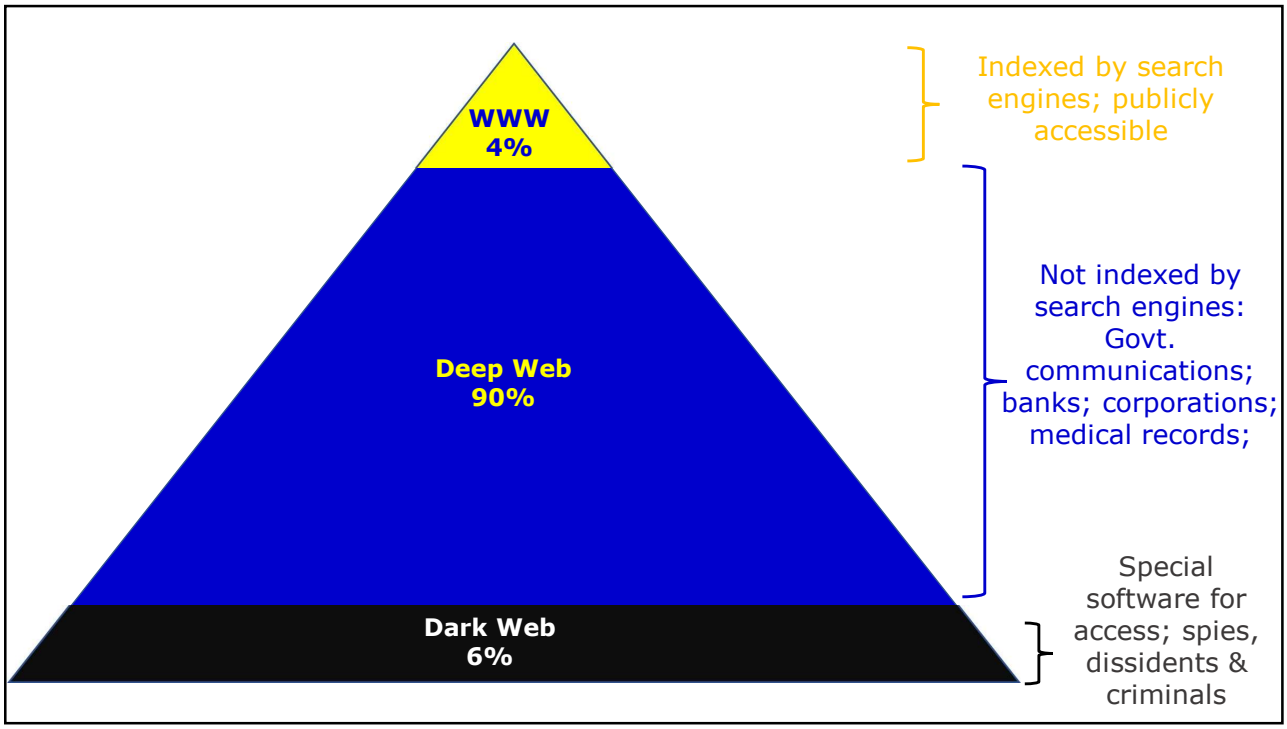
Internet, a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect. Sometimes referred to as a "network of networks"

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

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

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

2



3

Data, data everywhere

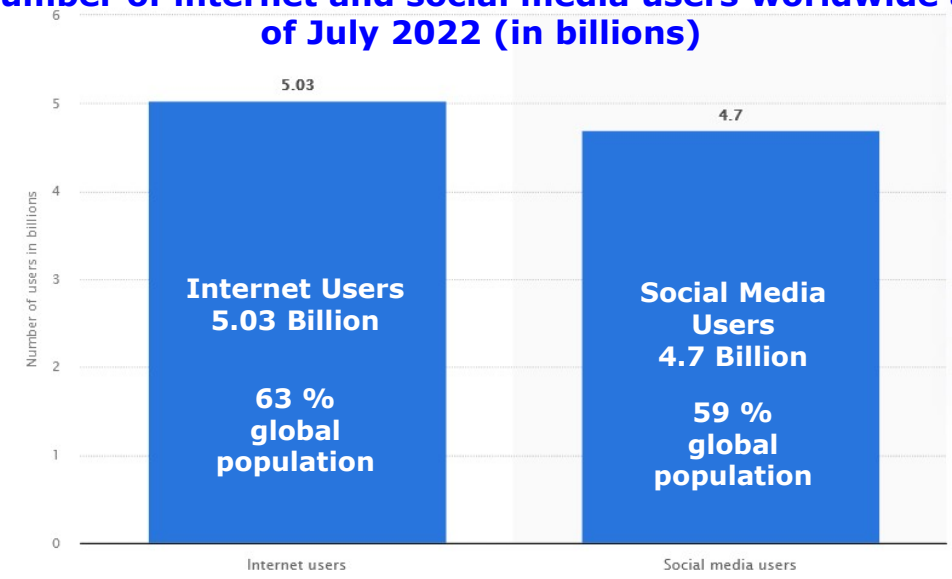
4.66 billion active internet users worldwide
= 59.5 % global population.
(Jan 2021)

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

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

4

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



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

5

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

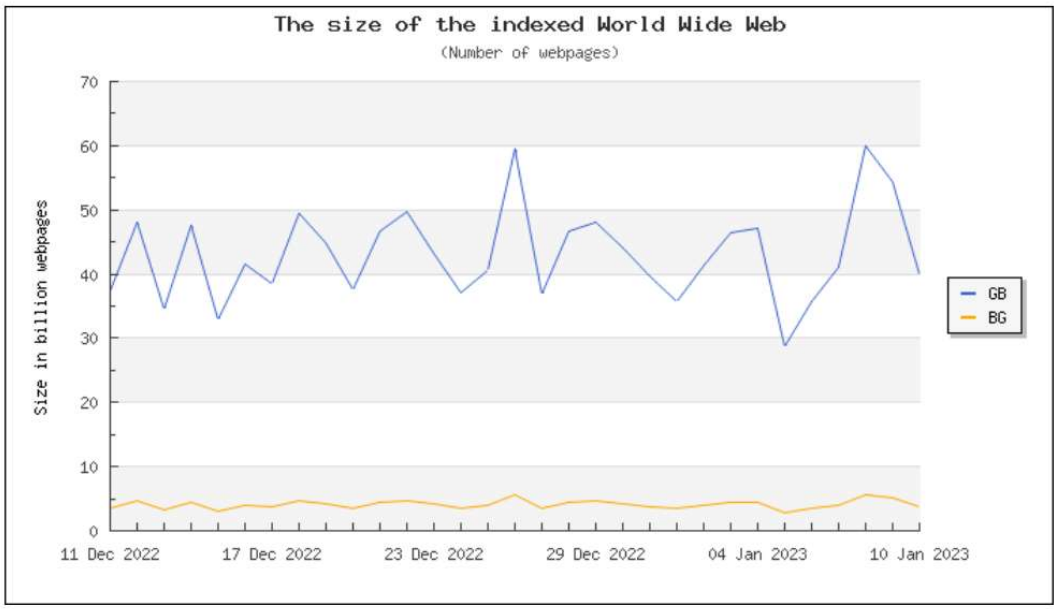
?

WWW contains **at least 3.81 billion pages**
Jan 2023
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

6



GB = Sorted on Google and Bing

BG = Sorted on Bing and Google

https://www.worldwidewebsize.com/

7

The Internet?

Insecure by design

8

Must prove:

Which device used in the offence

AND

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

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

Identifiers have been redacted

9

Protocols:

(In computing) = agreed way of doing something

IP
Internet Protocol

TCP
Transfer Control Protocol

UDP
User Datagram Protocol

FTP
File Transfer Protocol

DNS
Domain Name Service

10

TCP Transfer Control Protocol	UDP User Datagram Protocol
Slower	Faster
Requires a connection between sender/receiver	No connection required
Data sent in sequence & verified	No verification
Missing or incomplete data retransmitted	Missing data not replaced
Email, Web Browsing, FTP	Streaming, VOIP

11

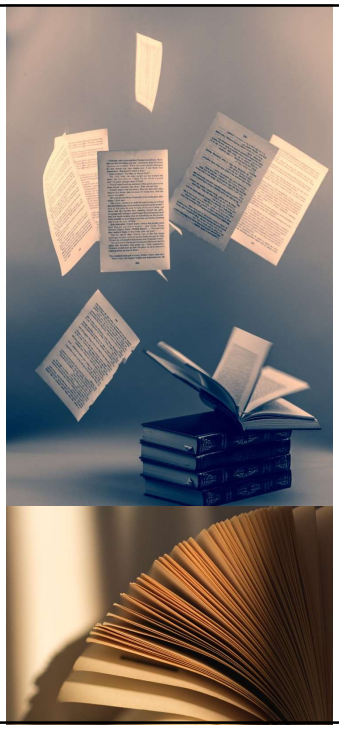
HTTP & HTTPS
(Hyper Text Transfer Protocol (Secure))

Indexed 'pages'

Collection of pages = Website

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

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



12

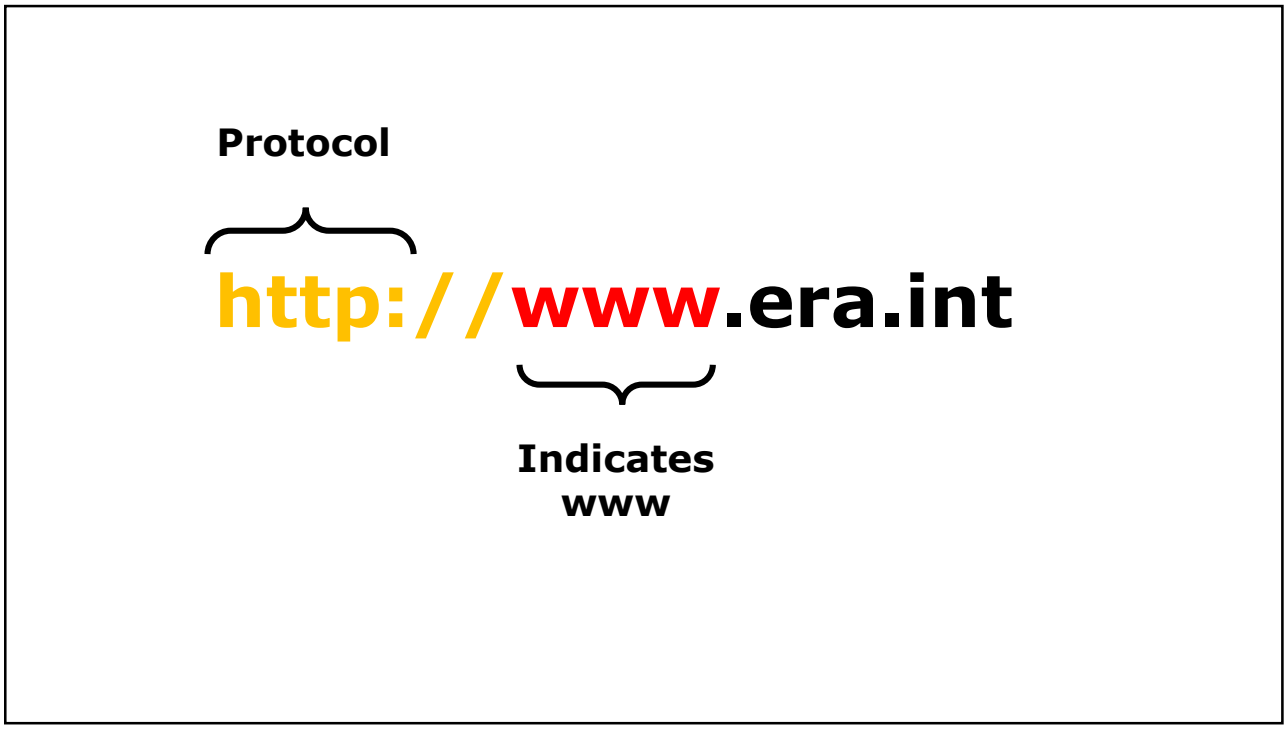
http://www.era.int

13

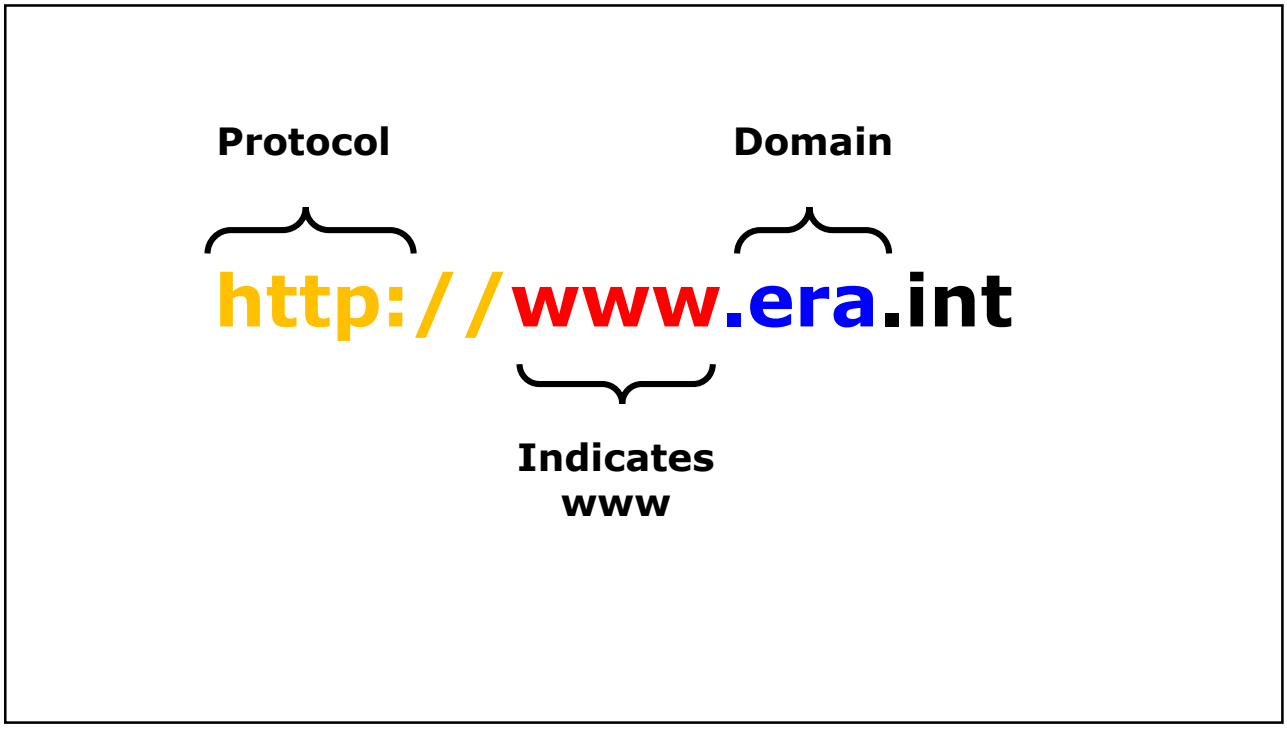
Protocol

http://www.era.int

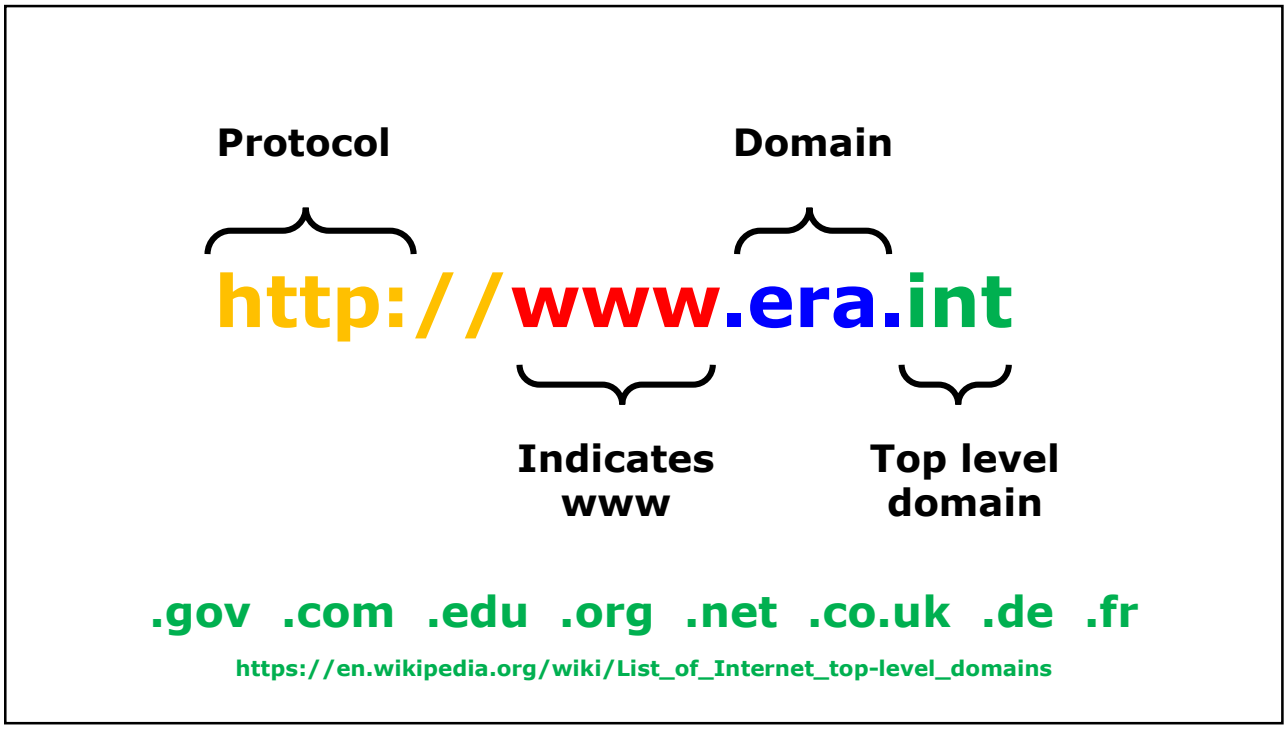
14


Protocol
http://www.era.int
Indicates
www

15


Protocol
Domain
http://www.era.int
Indicates
www

16



17

Whois

Register of Internet domain name 'owners'

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

(Authorised groups still have access)

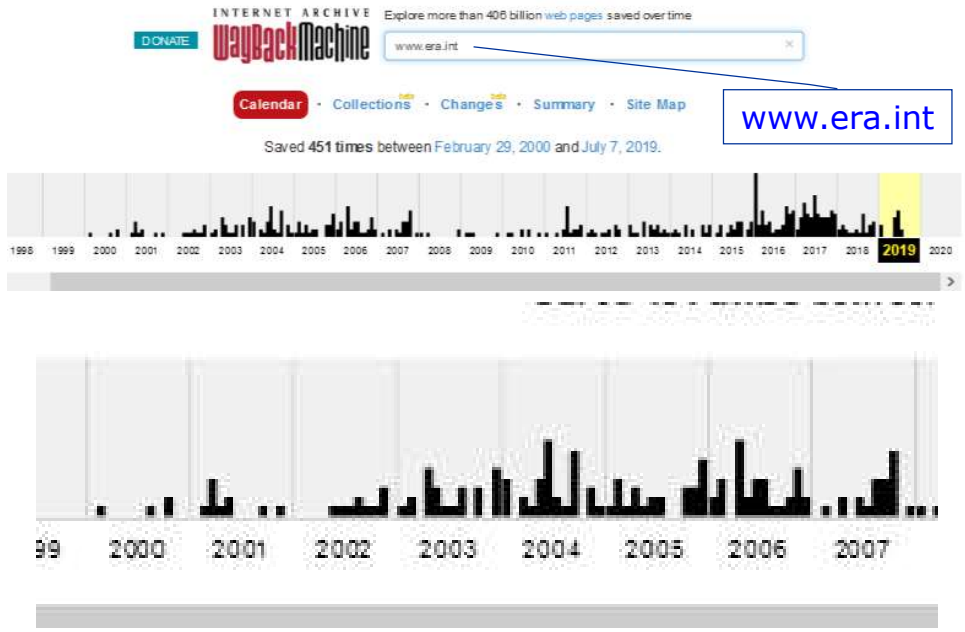
18

When websites change:

INTERNET ARCHIVE
WayBackMachine

(http://web.archive.org)

19



20

21

Website from 23 June 2000

22

Normally:
First step is to
the IP A

Can be faked, hidden or 'borrowed'

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

23

Internet Protocol (IP) Addresses

Two types:

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

Two versions:

IPv4

(4.3 billion - not enough numbers for everyone)

IPv6

What's yours? www.ipchicken.com

24

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

www.era.int

IPv4:

195.243.153.54

IPv6:

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

25

IP Address:

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

ISP holds records of usage

26

Be careful what you ask for …

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

27

UK Information Commissioner's Report 2016

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

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

28

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

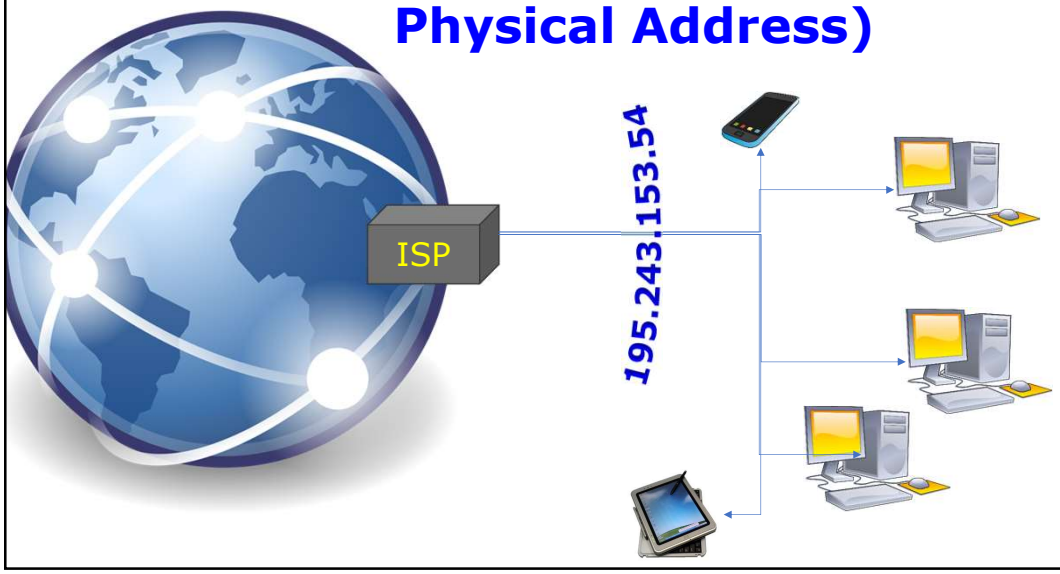
"When sending this information to the CSP, a transposition error changed the day and month"

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

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

29

MAC Address: (Media Access Control or Physical Address)

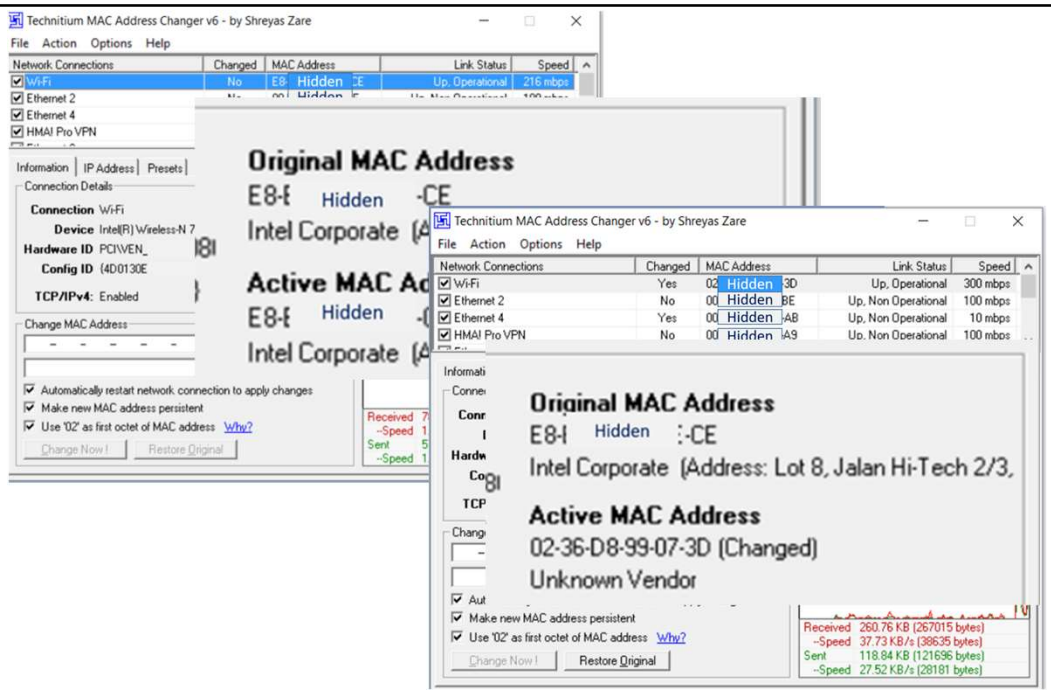


30

MAC Address

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

31



32

Phones - IMEI

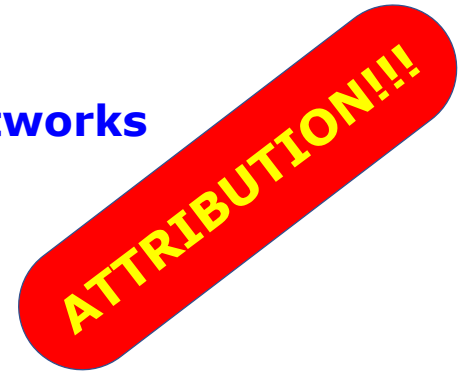
International Mobile Equipment Identity

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

33

Hiding an IP

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



34

4 March 2015, California

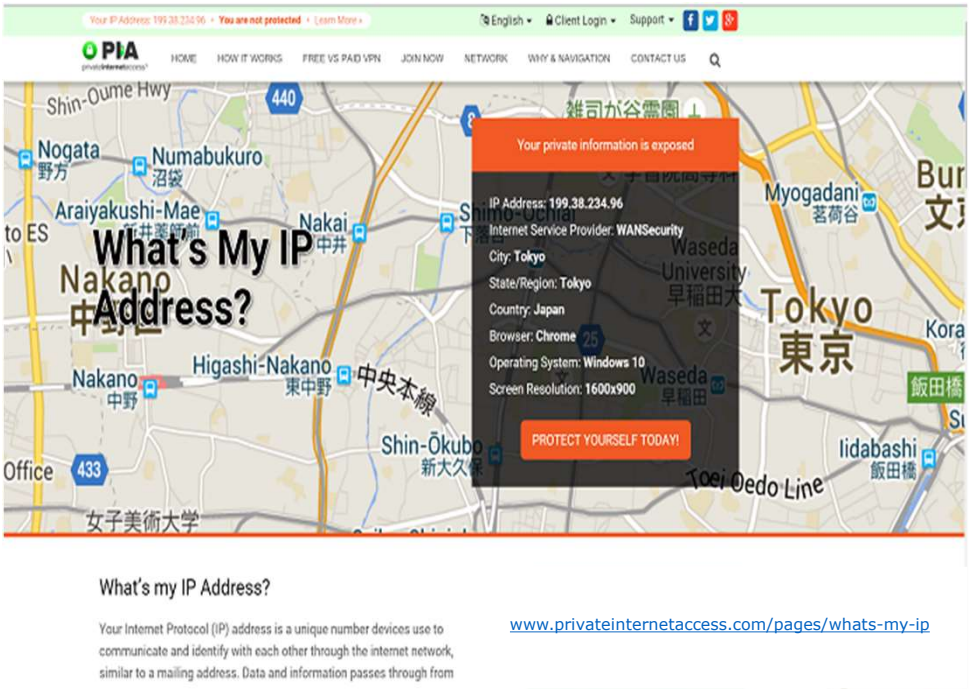
- **Home burgled**
- **65-inch Smart TV (with Netflix) stolen**
- **Victim realised someone using her Netflix account**

35

Bobby Alexander

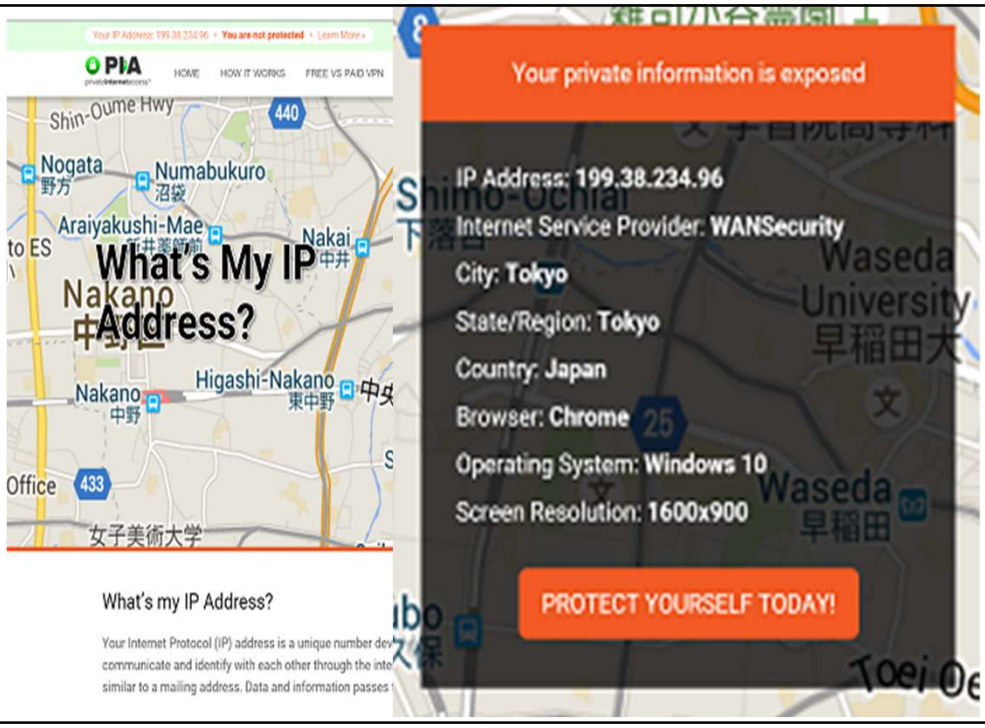
- **Police obtained IP address**
- **Raided the given address**
- **Came up with nothing**
- **Owners explained neighbour used their wifi account**

36



www.privateinternetaccess.com/pages/whats-my-ip

37



38

Virtual Private Networks (VPNs)

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

VPNs can be used by criminals to hide their location

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

39

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

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

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

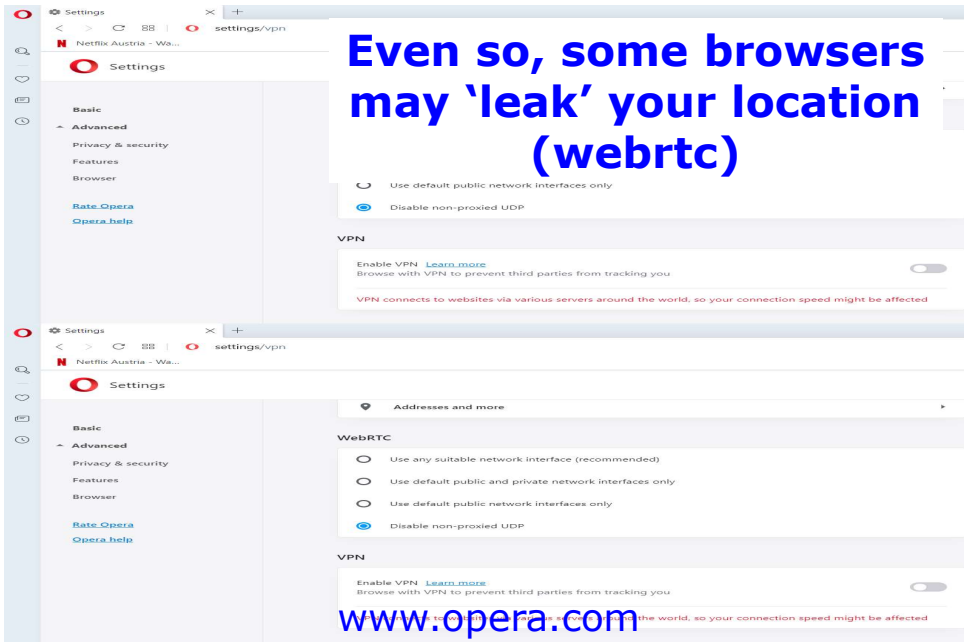
40

Well known VPN providers:

ExpressVPN
NordVPN
Hidemyass
CyberGhost VPN
Proton VPN

Included in some anti-virus/internet security packages

41



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

www.opera.com

Settings/Advanced/Privacy & security/

42

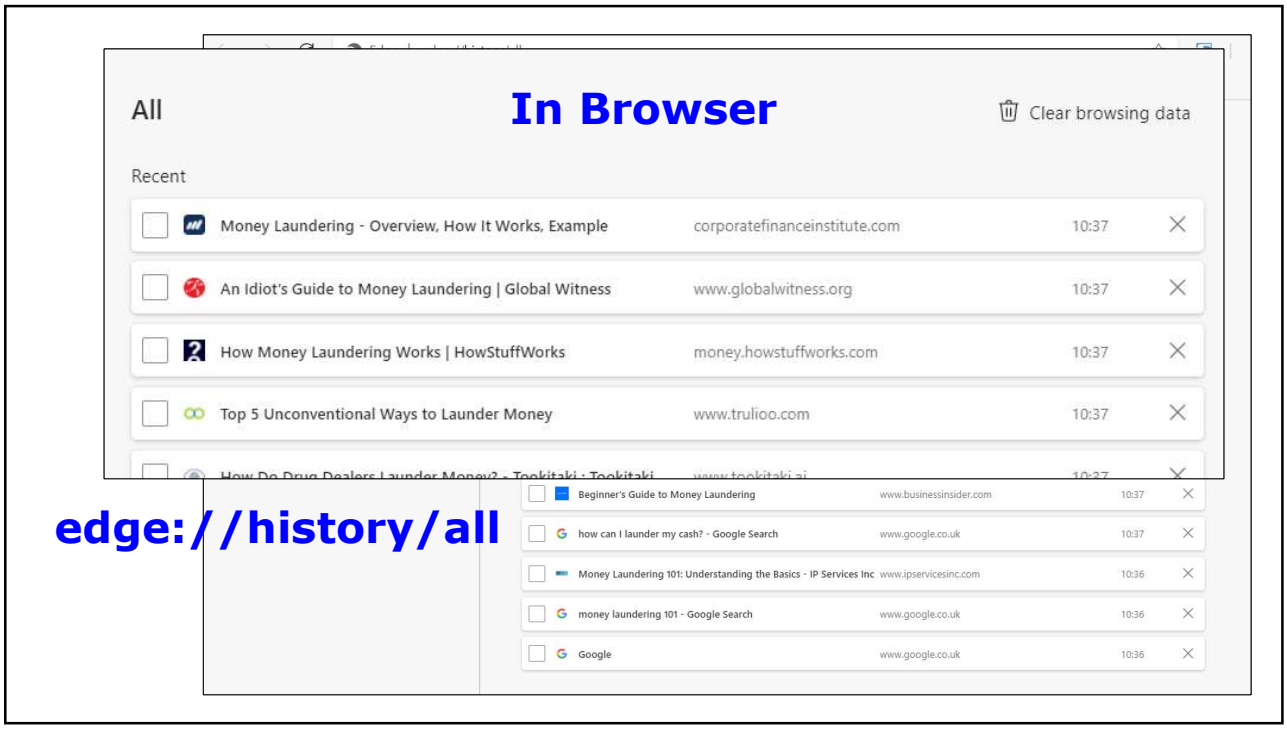
All you need is logs

43

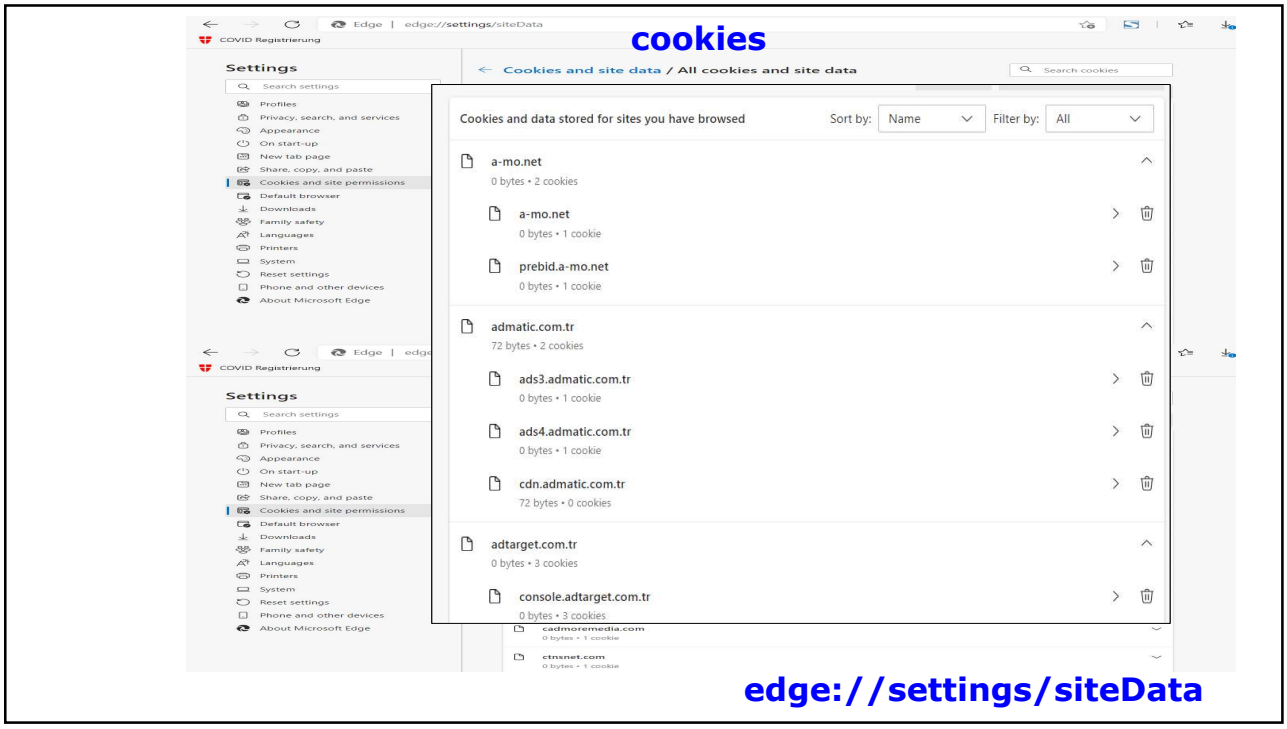
LOGS

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

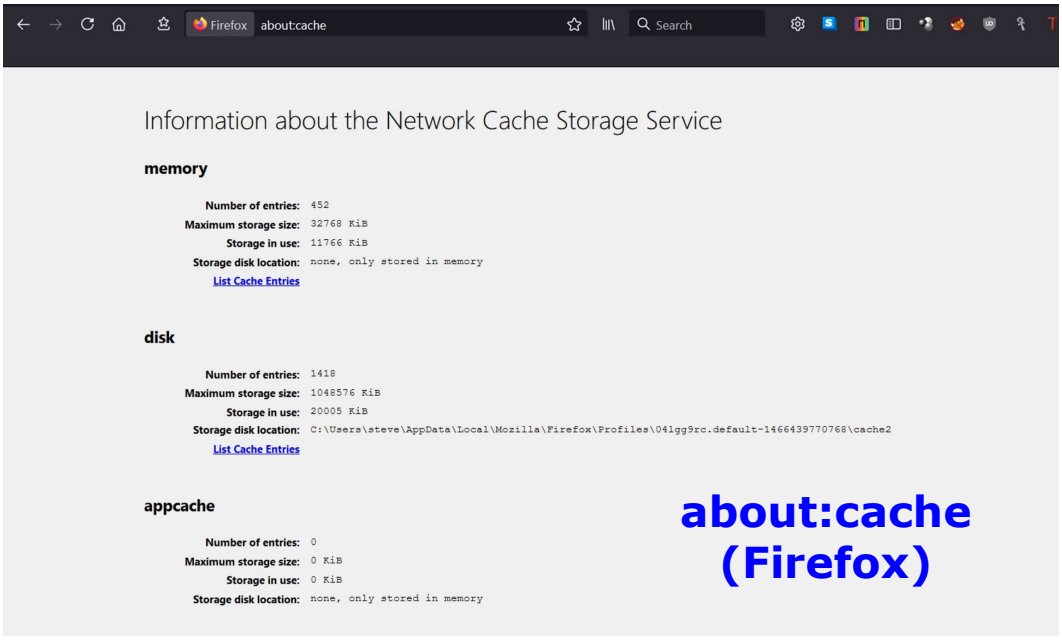
44


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

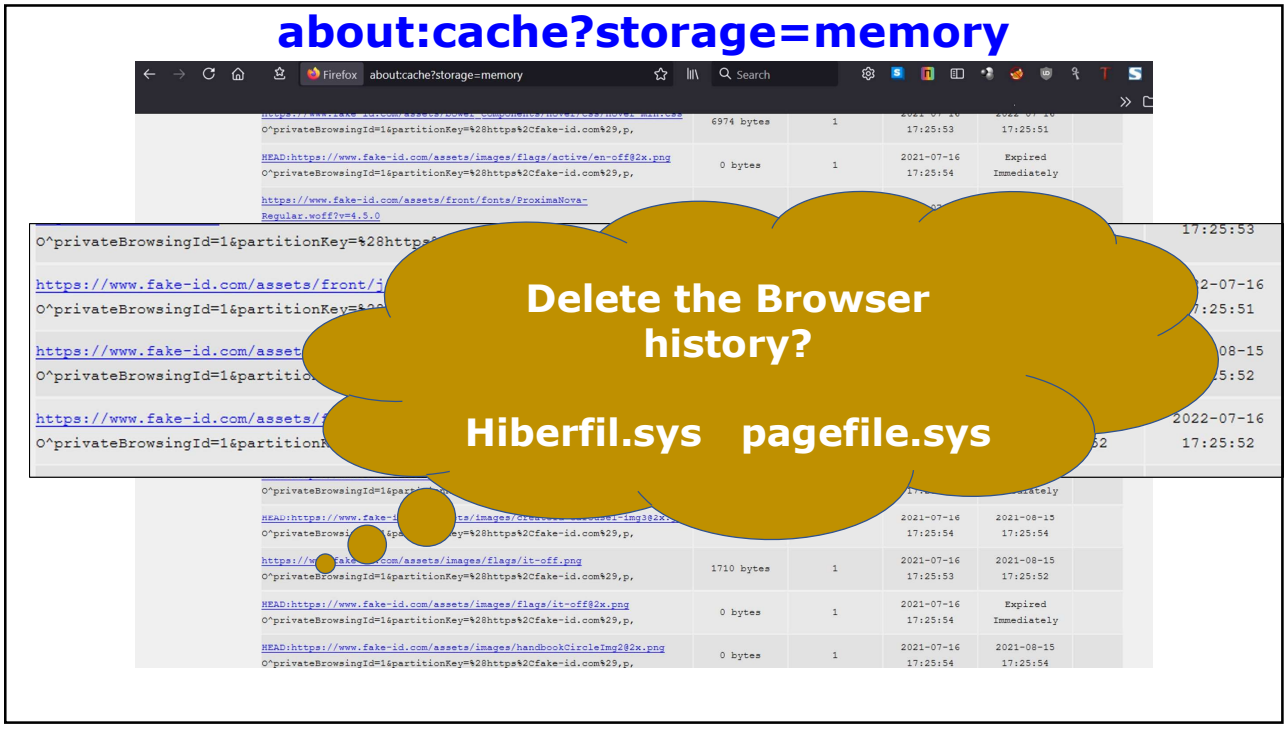
45


cookies
Settings
Cookies and site data / All cookies and site data
Cookies and data stored for sites you have browsed
Sort by:
Name
Filter by:
All
a-mo.net
0 bytes • 2 cookies
a-mo.net
0 bytes • 1 cookie
prebid.a-mo.net
0 bytes • 1 cookie
admatic.com.tr
72 bytes • 2 cookies
ads3.admatic.com.tr
0 bytes • 1 cookie
ads4.admatic.com.tr
0 bytes • 1 cookie
cdn.admatic.com.tr
72 bytes • 0 cookies
adtarget.com.tr
0 bytes • 3 cookies
console.adtarget.com.tr
0 bytes • 3 cookies
edge://settings/siteData

46


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

47


about:cache?storage=memory
Firefox
about:cache?storage=memory
Search
Delete the Browser history?
Hiberfil.sys
pagefile.sys

48

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

Username weirdos 0000

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

Encrypted chats discussed with seller:

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

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

49

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"

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

50

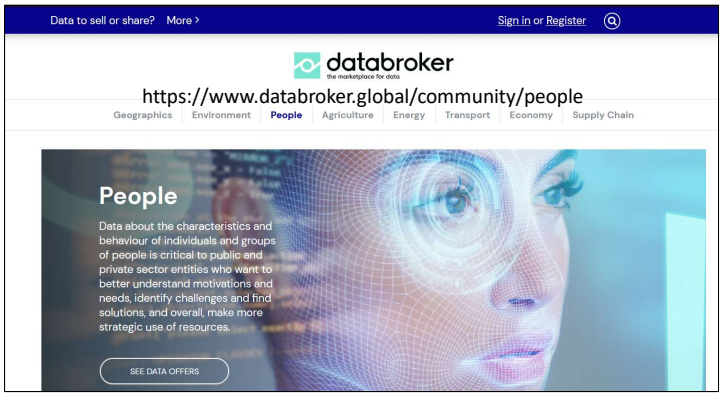
Cookies, search history and device configuration create a characteristic 'browser fingerprint'

Try this out:

https://webkay.robinlinus.com/

51

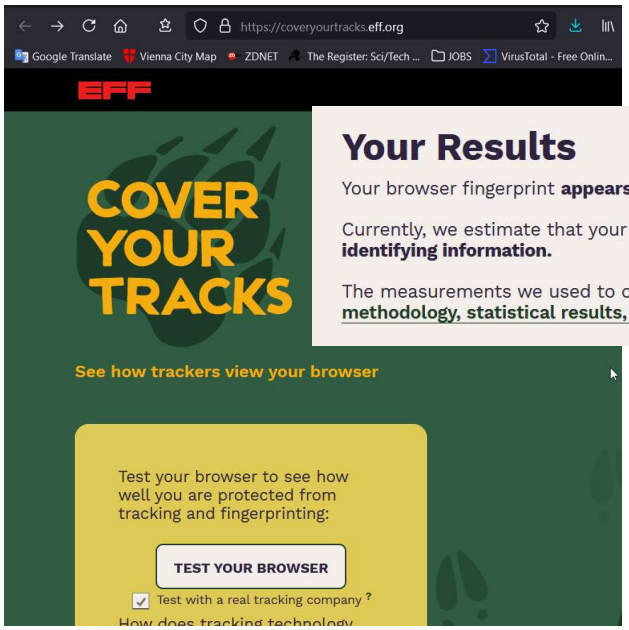
Commercial value – profile used by Data Brokers for targeted online advertising.



'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.'

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

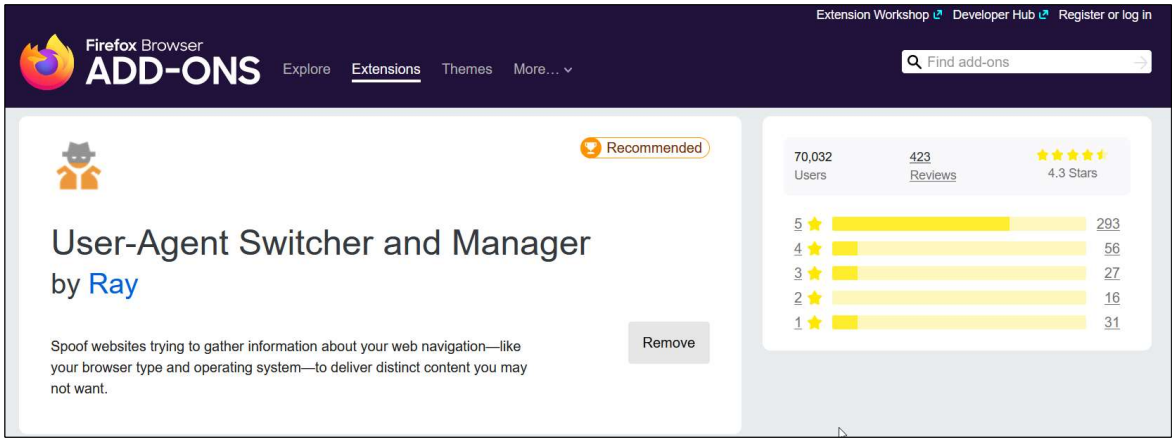
52



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

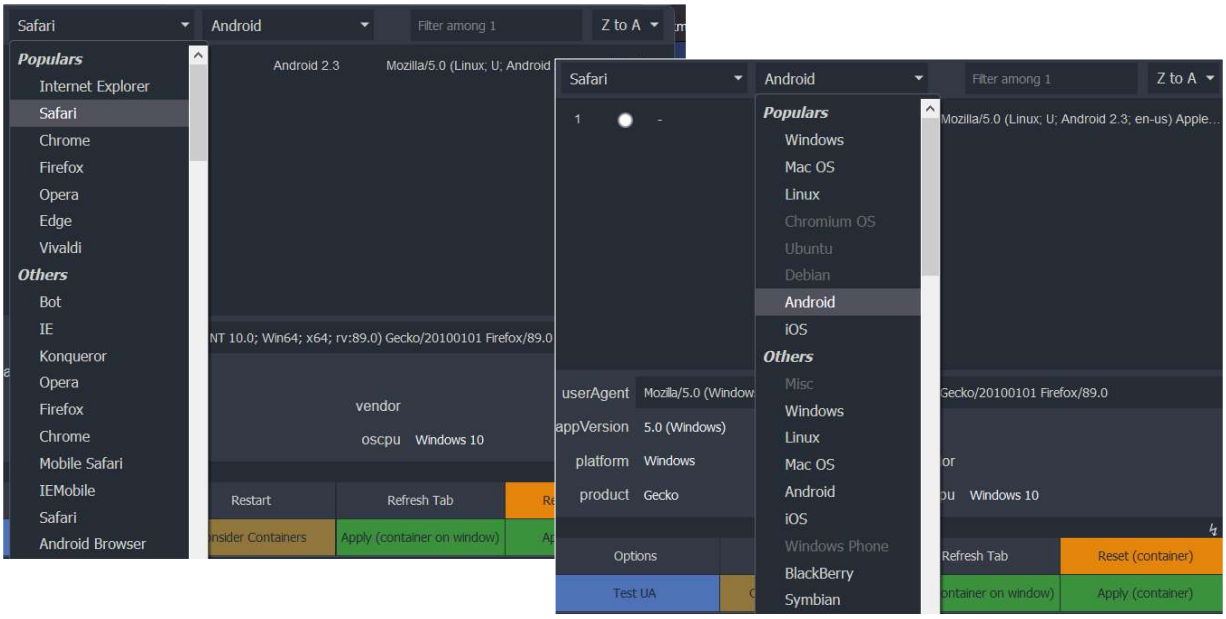
53

Browser fingerprint can also be faked:



54

Browser fingerprint can also be faked:



55

Your data may be spread across servers in multiple jurisdictions

Your data stored & processed somewhere else

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

The Cloud

Outsourcing: Iaas, Paas, Saas

Relocated for business reasons (like load or electricity prices)

Even Cloud provider may not know where it is

Problems getting evidence:

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

56

IOT

Estimated 22 billion - 50 billion devices

All connected

All generating & logging data

57

IOT

How secure are they?

Default passwords

Most lack built-in security

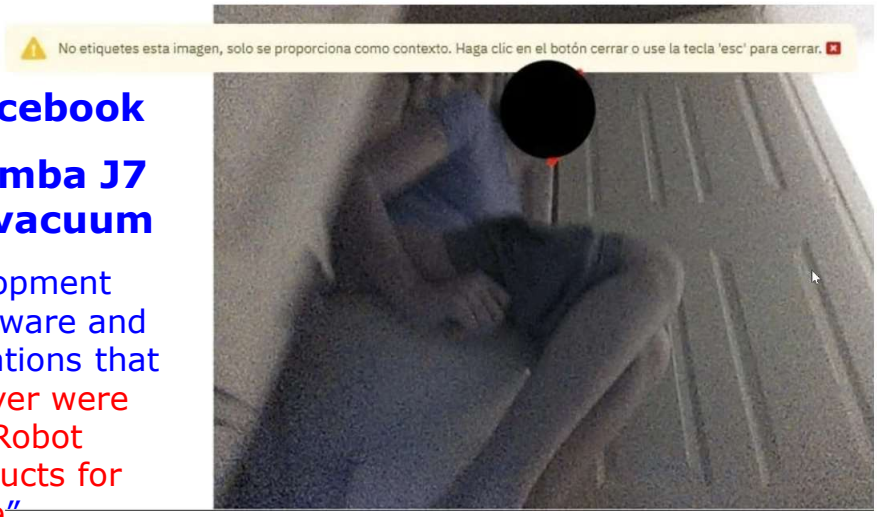
https://www.zdnet.com/article/your-insecure-internet-of-things-devices-are-putting-everyone-at-risk-of-attack/

58

Posted to Facebook

iRobot's Roomba J7 series robot vacuum

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



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

59

Meta-Search Engines

www.metacrawler.com

metager.org

www.wolframalpha.com

www.dogpile.com

www.startpage.com

60

61

No central control

All websites end with .onion

Can be used to access DarkNet

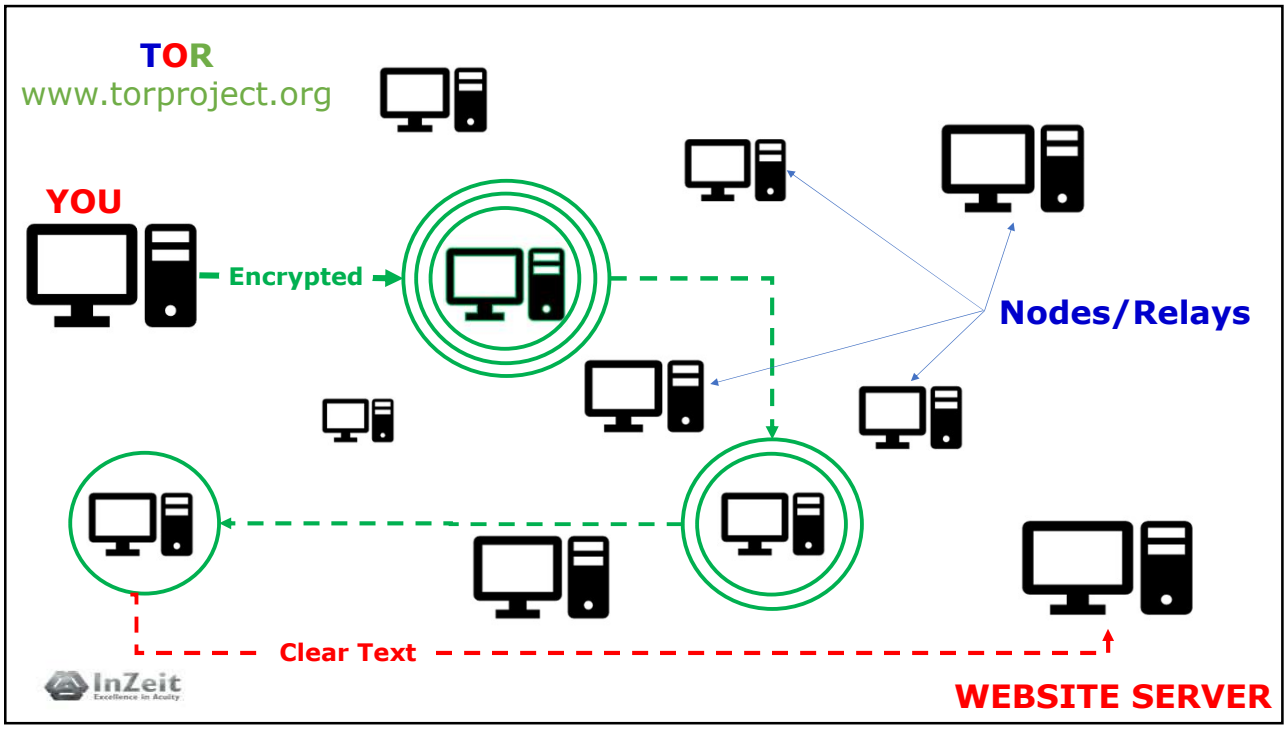
TOR
The Onion Router

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

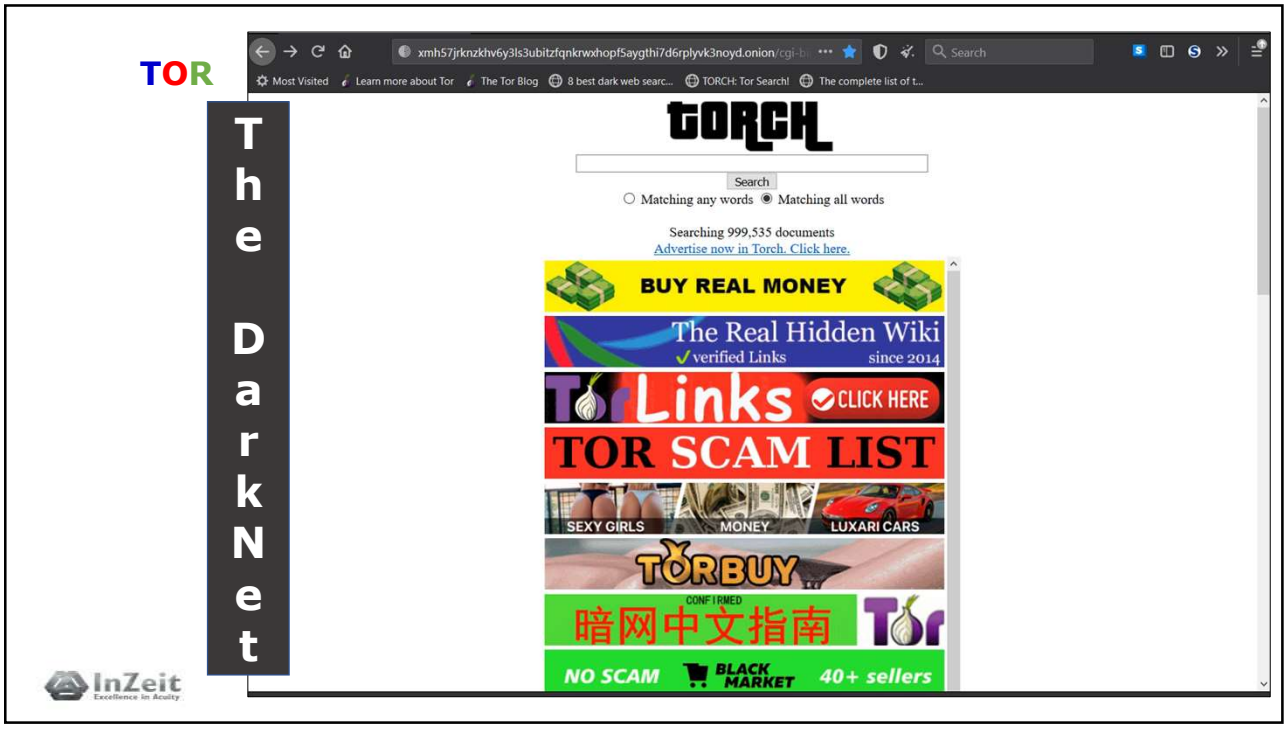
'Anonymising technology' (there are others)

InZeit

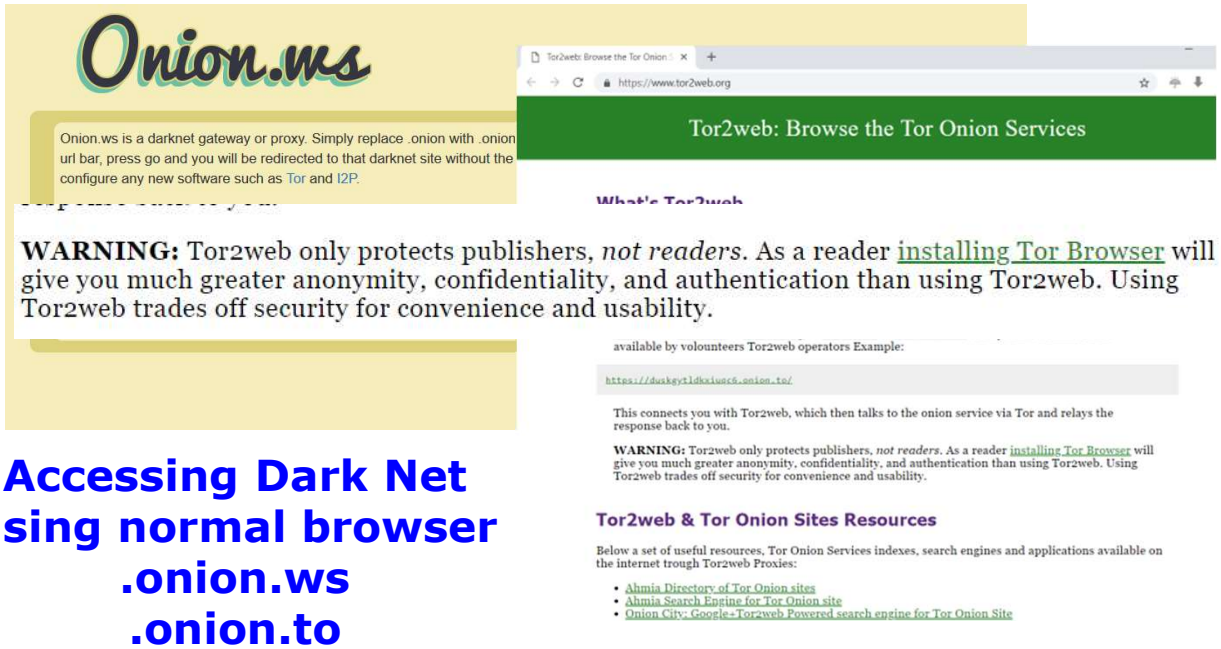
62


TOR
www.torproject.org
YOU
Encrypted
Nodes/Relays
Clear Text
InZeit
WEBSITE SERVER

63

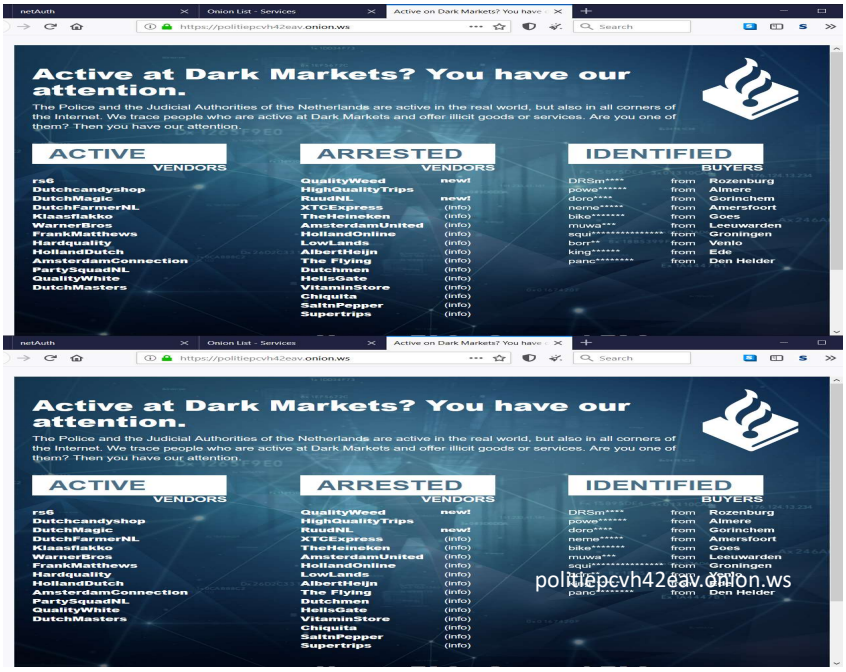

TOR
The DarkNet
TORCH
Search
Matching any words
Matching all words
Searching 999,535 documents
Advertise now in Torch. Click here.
BUY REAL MONEY
The Real Hidden Wiki
verified Links
since 2014
TorLinks
CLICK HERE
TOR SCAM LIST
SEXY GIRLS
MONEY
LUXARI CARS
TORBUY
CONFIRMED
暗网中文指南
NO SCAM
BLACK MARKET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

64

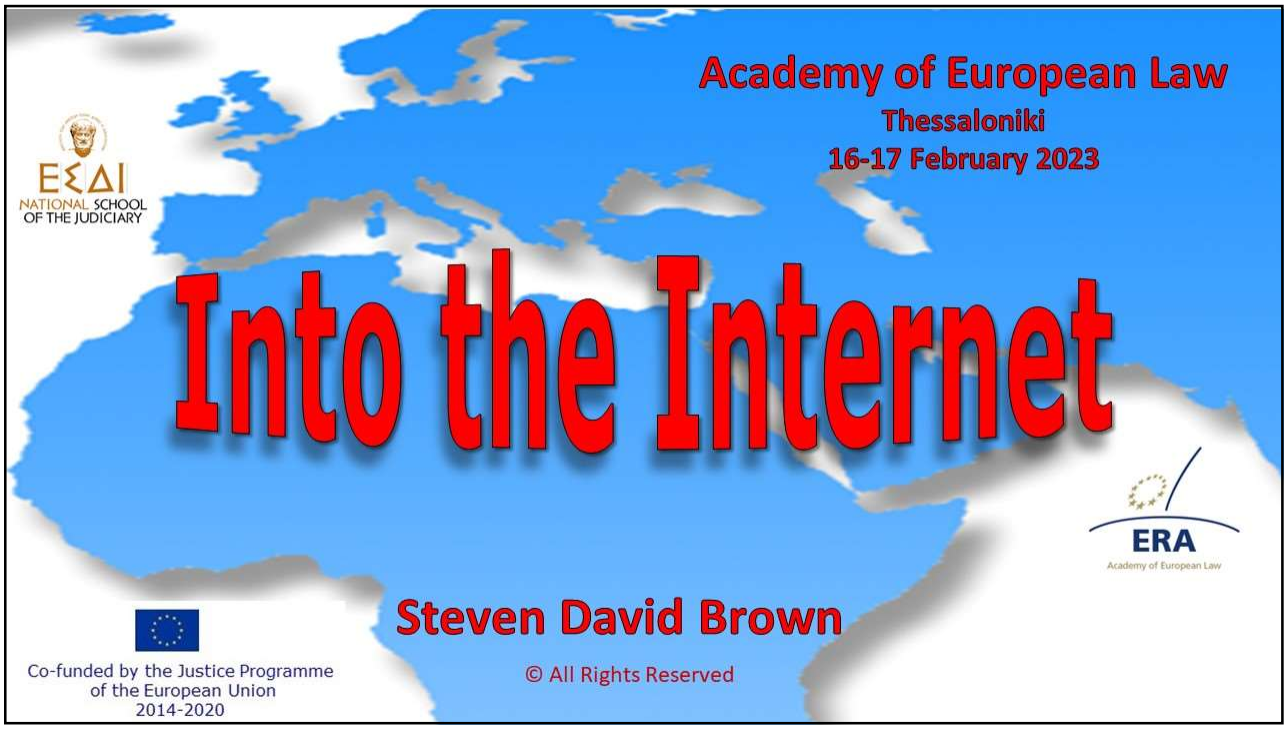


Accessing Dark Net using normal browser
.onion.ws
.onion.to

65



66



67

Resources and further reading

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

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

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

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

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

68

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

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

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

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

69

Your Browser Logs
(Enter in address bar of browser)

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

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

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

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

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

70

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

Internet of Things
Palmer,D. (2021) Your insecure Internet of Things devices are putting everyone at risk of attack https://www.zdnet.com/article/your-insecure-internet-of-things-devices-are-putting-everyone-at-risk-of-attack/
Guo,E. (2022) A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook? https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

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

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

71

Open Source Intelligence

OSINT Tools

Bilal Şen

Senior Investigator

With financial support from the European Union

www.coninsec.com

1

TABLE OF CONTENT

Open Source Intelligence

2

COMMON OSINT USAGE

It is not hacking

It is not invented by law enforcement

It is not always 'free'

It is not just the internet

It is not something the subject/s cant do

It is not as easy as we think it is

It is not only for justice and security

Publicly available?

May require verification

Reconnaissance (Hacking)

PenTest (Cyber Security)

Due Diligence (Company Accusation)

Investigation (Crime or Dispute)

Protection (Parents & Juveniles)

Research (Neighborhood Check)

Verification (CV Verification)

Defense (Military Monitor)

Academic (most of it)

Competition (Commercial Intelligence)

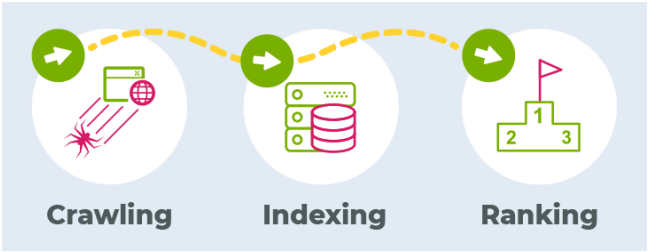
Any Means of Business

3

VERIFICATION

4

GOOGLE SEARCH PROCESS



5

WHICH GOOGLE IS BEST FOR YOU?

6

GOOGLE LOCAL COPY SEARCH TEST

Search Engine Address	Search Term	Amount of Hits	With VPN Connection (Location CA, USA)
Google.de	bilal sen	14.6 M	13.9 M
Google.com.tr	bilal sen	27.7 M	8.8 M
Google.com	bilal sen	7.7 M	13.9 M
Google.com	bilal şen	11.7 M	

7

GOOGLE SEARCH VARIANTS TEST

Google Search Variants Test

Test Time : 07.02.2022 09:15 - 10:30
Test Default Location : Germany
Operation System : Windows 10 English
Browser : Chrome,
Scrape Tool : Instant Data Scraper Chrome Extension
Search Term : Undisclosed

	Search Engine	Location	Search Term	Scraped Rows
1	Google.com	Germany	...	111
2	Google.it	Italy VPN	...	101
3	Google.be	Germany	...	99
4	Google.de	Germany	...	127
5	Google.fr	France VPN	...	97
6	Google.co.uk	UK VPN	...	103
7	Google.com	Singapore VPN	...	109
8	Google.com Image	Germany	...	503
9	Google.com News	Germany	...	291
10	Google.com Books	Germany	...	635

8

DON'T FORGET ROBOT.TXT

```
User-agent:  *
Disallow: /cgi-bin/
Disallow: /wp-admin/
Disallow: /wp-content/
Disallow: /wp-includes/
Disallow: /recommended/
Disallow: /comments/feed/
Disallow: /trackback/
Disallow: /index.php
Disallow: /xmlrpc.php
Disallow: /wp-content/plugins/

User-agent: NinjaBot
Allow: /

User-agent: Mediapartners-Google*
Allow: /

User-agent: Googlebot-Image
Allow: /wp-content/uploads/

User-agent: Adsbot-Google
Allow: /


User-agent: Googlebot-Mobile
Allow: /
```

→ Will always be ignored by the Search Engin bots.

9

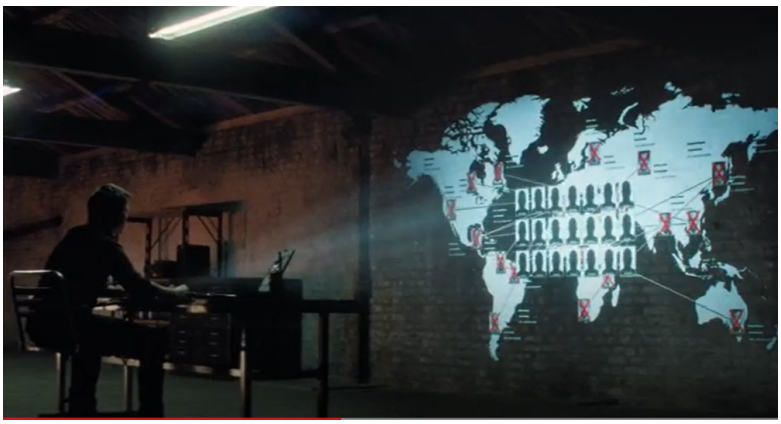
MOST HELPFUL AND ALREADY KNOWN SEARCH OPERATORS

Operator	Usage
site:	Show only the results from a certain website; e.g. site:mangools.com
" "	Limit the results to the ones containing the exact phrase in the quotation marks; e.g. "Google Keyword Planner alternative"
OR	This will show results for *keyword1* or *keyword2* or both. Can be substituted with the vertical pipe (|); e.g. mango OR banana, mango | banana
–	Exclude the term (or a whole operator) by putting the minus symbol in front of it; e.g. king kong director -jackson
*	Acts as a wild-card character that will match any word or phrase; e.g. most popular * in the world
intitle: allintitle:	Only shows results that include (all) the searched words in the title; e.g. allintitle:best toys for 2 year olds
inurl: allinurl:	Only shows results that include (all) the searched words in the URL; e.g. inurl:seo
Filetype/ext	Look only for a specific filetype (PDF, DOCX, TXT, PPT, etc.); e.g. filetype:PDF

10

YOUR TASK

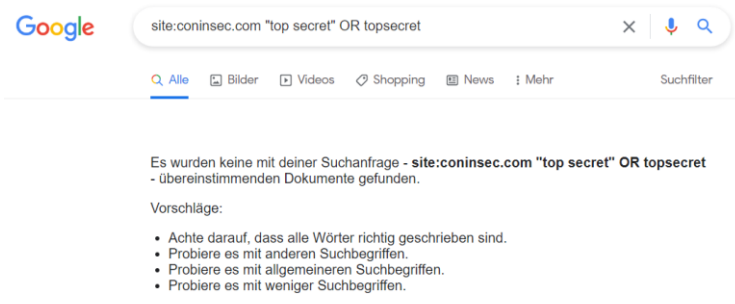
Find a top secret file and a crucial message of Coninsec



11

EXAMPLE SEARCH 1

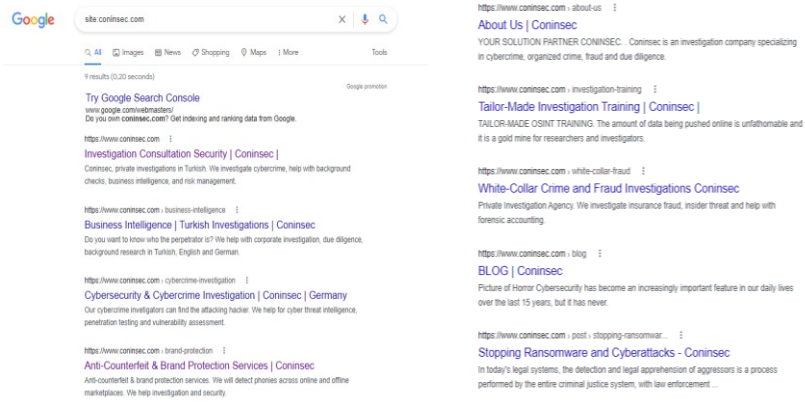
⑩ **site:coninsec.com "top secret" OR topsecret**



12

EXAMPLE SEARCH 2

site:coninsec.com



13

DIFFERENT APPROACH

14

ARTIFICIAL INTELLIGENCE & OSINT

15

DATA COLLECTION SOURCES

- Maps, Satellites & Streetview
- Location Based Searches
- Image & Video Verification
- Social Media
- Transportation
- Date & Time
- WhoIs, IPs & Website Analysis
- People & Phone Numbers
- Archiving & Downloading
- Company Registries
- Data Visualization
- Online Security & Privacy
- Finding Experts
- Miscellaneous
- Guides & Handbooks

16

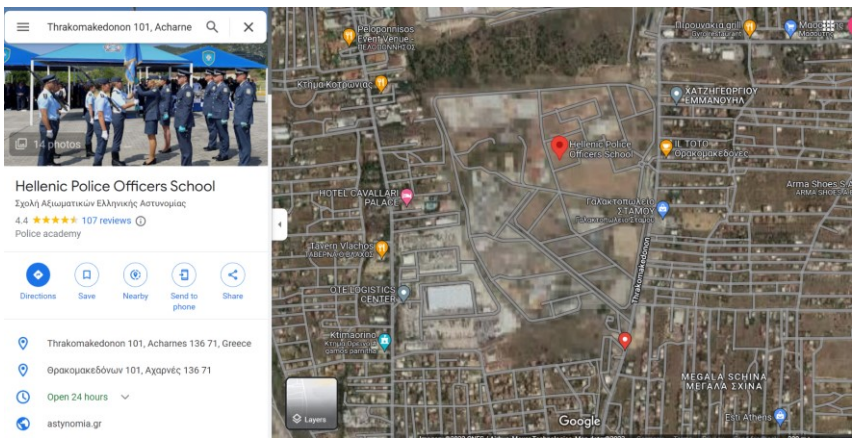
ALERT MANAGEMENT

Creating and managing search alerts is a passive and automated information gathering process that helps to collect timely and updated information.

17

ALTERNATIVE COULD BE BETTER

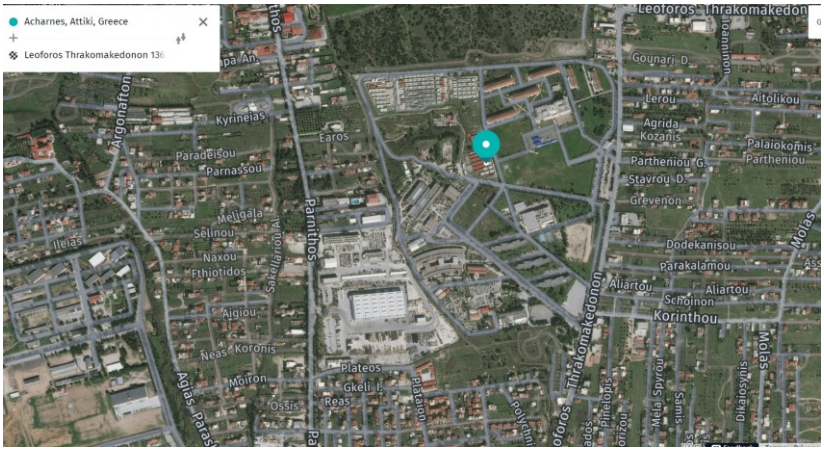
GOOGLE MAP RESULTS



18

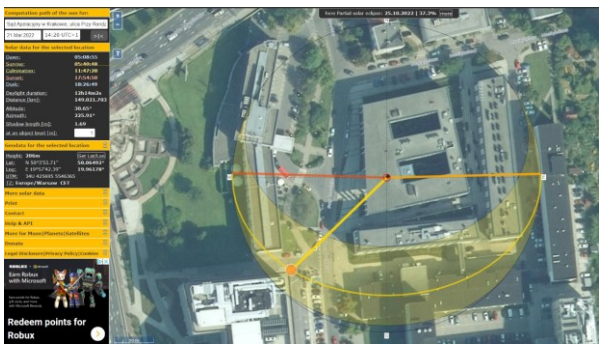
ALTERNATIVE COULD BE BETTER

wego.here.com



19

suncalc.org

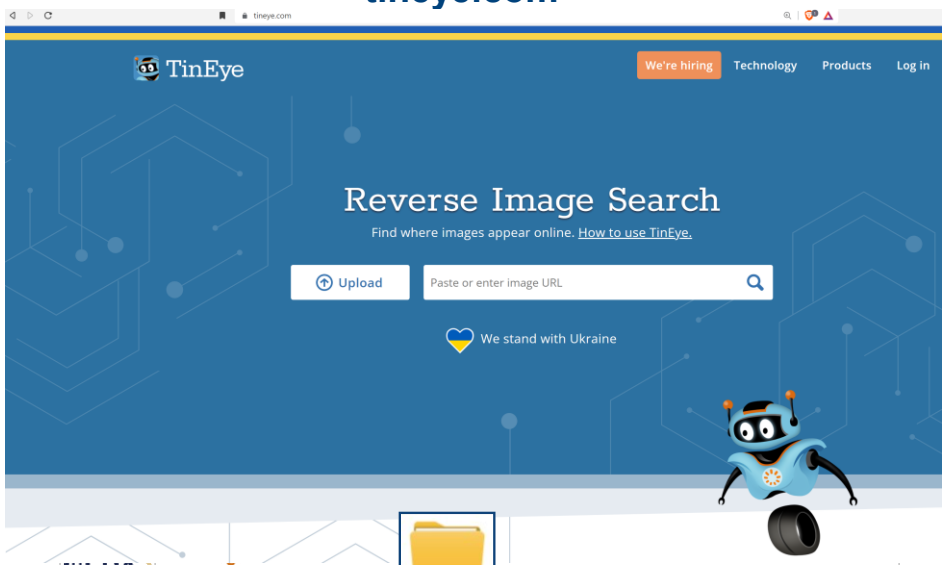


The SunCalc is a sunlight calculator. It helps determine time and date by sun movement and sunlight analysis during the given day at the given location.

www.suncalc.org/#/50.0649,19.9618,19/2022.03.21/14:20/1/1

20

tineye.com



21

Live OSINT Case Demonstration

22

QUESTIONS & DISCUSSION

Bilal Şen

bs@coninsec.com

Handling electronic evidence on mobile devices in court: experiences in Greece

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

Sapfo Katsanaki
Public Prosecutor
SNE to EPPO
LLM IT Law (London)
LLM Penal Sciences (Athens)*

Thessaloniki, 16-17 February 2023

*The views and opinions expressed in this presentation are those of the speaker and do not necessarily reflect the views or positions of the EPPO.

1

What is e-evidence and why is it so important?

Definition ➡ all kind of evidence regardless of its origin, namely both evidence originally born electronically as well as evidence of any form, either physical or analogue, that is then digitised and acquires a digital status. (For the definition of e-evidence see the EVIDENCE Project—Deliverable 2.1—EVIDENCE Semantic Structure, 24 http://www.evidenceproject.eu/the-activities/deliverables.html)

- More and more crimes committed online and facilitated by electronic devices such as mobile devices traces of the crimes are left on these devices

HOWEVER, e- evidence is

- Intangible
- Ephemeral
- Volatile/ Subject to easy movement and manipulation by computers
- Hard to locate

2

E - evidence on a mobile device (a non - exhaustive list)

3

Electronic evidence under Greek Law

- Article 13 of Penal Code → Broad definition of digital data (art.13z) and electronic document (art.13c)
- Mobile device has a CPU, memory, batteries, input interfaces such as a keypad or mouthpiece, and output interfaces such as a screen or earpiece → equitable to a pc
- Examples from case Law
  - The sms is an electronic document (8/2019 First Instance Mixed Court of Heraklion, Crete)
  - Mobile devices should be considered as PCs (8/2019 First Instance Mixed Court of Heraklion, Crete)
  - Evidence brought before Courts: Photographs/videos found on a pc/mobile phone (Supreme Court 1982/2008, First Instance Judicial Council of Athens 428/2015 First Instance Judicial Council of Arta 50/2015) and lists of calls stored on the SIM card (Judicial Council of Rodopi 108/2004)
  - Digital discs, where conversations are recorded, constitute admissible evidence and specifically documents. Their hearing during trial constitutes an appropirate technical method of reading them.(Areios Pagos 166/2021).

4

Seizure of Digital Data
Procedure laid down in Article 265
of New Criminal Procedure Code
(entered into force July 2019)

Provisions for the seizure of

- ✓a computer system or part of it and computer data stored therein
- ✓ a computer-data storage medium in which computer data may be stored
- ✓a remote computer system or part of it and computer data stored therein or in a remote computer-data storage medium, interconnected to the computer system to which the person conducting the investigation has physical access.

5

Procedure of seizure

Seizure is imposed with the use of appropriate equipment which permits:

- Removal and Seizure of the medium where data is stored
- Copy and extraction of the data stored
- Reproduction and verification of the authenticity and integrity of the data seized

6

After the seizure (Art.265 para 4-6 Criminal Procedure Code)

- ✓ During criminal procedures digital data seized remains stored in a data storage medium, which is included in the case file.
- ✓ A safe copy of this data storage medium is kept by the office of exhibits of the Court to ensure retrieval in case of damage/loss.
- ✓ Accessibility and reproduction of the data seized is strictly controlled and protected (by encryption/use of passwords).
- ✓ Seized data can only be copied, following the prior authorization of the Court, the prosecutor, or the investigating judge in order to be used in another case.

2/2020 Order of the Investigating Judge of Aigio: The accused's application to receive a copy of the digital data extracted from his computer during a seizure according to Art.265 CCP is rejected, as no such right is provided under para.5 and 6 of this Art.

7

Who examines and analyses digital data?

The Forensic Science Division of the Hellenic Police is the National Forensic Service of Greece

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=90090&Itemid=274&lang=EN

Digital data is examined and analyzed by the Digital Forensic Department and the results of the analysis are documented in a report (Art.30 para 10 Presidential Decree 14/2001).

Opinion 6/2021 of the Prosecutor of the Supreme Court on the seizure of digital data: The report drafted by the expert personnel of the Digital Forensic Department with the use of proper equipment, regarding the collection, extraction, analysis, reproduction, authentication and verification of the data is an *expert opinion*, the conclusions and results of which constitute an indivisible part of the report for the seizure of the physical carrier.

8

Rights of the suspect/accused person

- Be present during the research and seizure of digital data
- Appoint a technical consultant who has the right to be present during the examination of the evidence, comment on the findings of the report of the Digital Forensic Department and draft a report with his / her proper findings (art.204,207,208 Criminal Procedure Code) ➡ **Violation** of this right is considered a violation of the rights of defense, as provided under Art. 171 par.1d Criminal Procedure Code and thus nullity is implied which can be claimed by the accused/suspected or be taken into consideration by Court ex officio.

9

Case Law

- Three-member Air Force Court 137/2006: The defendant claimed that the messages in question appear to have been sent by his mobile with the use of the method of the caller ID spoofing and he invoked a report drafted by an expert appointed by him, analysing this method. The allegation was refuted on the grounds that the caller ID spoofing does not permit "biderectional" communication.
- Areios Pagos 241/2020: According to the report drafted by the expert personnel of the Digital Forensic Department the image files of child pornography found on the accused's mobile constitute snapshot's thumbnails of video files which were published in the website with adult pornography content, where the accused navigated through his mobile phone and they were stored therein because of the automatic caching function of the application for navigation, without the accused having the possibility to access those files and without any access to the videos having been detected ➡ Hence not enough evidence that the child pornography offence was commited.

10

What happens if you can't unlock the mobile?

- Article 19 par.4 of the Convention on Cybercrime has not been incorporated in Criminal Procedure Code.
- No mandatory key disclosure/mandatory decryption laws.
- If suspect/accused person is compelled to hand over cryptographic keys or to provide any assistance ➡ interference with the right against self-incrimination and the right to silence?

BUT see also Article 104 of the new Criminal Procedure Code

If assistance is required and denied by third parties (service providers)

⬇

Possible criminal liability for harboring the offender ?

11

Jurisdictional Issues

Access to extraterritorially located data

- Direct cooperation with service providers (esp. Request of an IP)
- Use of European Investigation Order
- Unilateral transborder access according to Art. 32 of the Convention on Cybercrime (ratified by L.4411/2016)

Second Protocol to the Budapest Convention already adopted

However more and more data is stored in the cloud
Where is the cloud???

12

Evidence from social networks

Judgment 8/2019 of First Instance Mixed Court of Heraklion, Crete

- Mobile phones should be considered computers
- sms is a form of distant communication and thus should be evalutated as a letter. Messages exchanged in social networks are admissible as evidence and do not violate the rights to free communications and to secrecy of communications when they are brought as evidence by either of the communicating parties. However, they would constitute prohibited evidence and would be inadmissible, if they are brought by a third party, who did not participate in the communication ➡ It was held that the conversations from messenger between the accused and the victim, brought by either of them, can be used as evidence.
- A photo constitutes personal data. However, if a photo is published in the Facebook profile and is accessible by everybody ➡ It can be used as evidence since no privacy right is violated.

Areios Pagos 954/2020

- The joined commission of a crime by the accused is proved, among others, by the content of their conversations through Facebook, which were printed and brought to Court as evidence.
- An allegation that the conversations were inadmissible as evidence was rightly rejected by the Court .
- The content of the communication is protected by the secrecy of communications while the communication takes place and the protection ends when the communication is ended. After the communication has been ended it is protected by the right to privacy and as personal data (art. 9 and 9A of the Constitution)

13

But taking evidence from mobile phones can constitute an offence

Three Member First Instance Court of Florina 396/2017

- sms messages stored in the mobile, after the completion of communication, are not protected by the secrecy of communications
- HOWEVER, they are protected by the right to privacy and as personal data (art. 9 and 9A of the Constitution)

Taking photos from the mobile's display, where the content of SMS messages is displayed, and bringing them to Civil Court as evidence can constitute the criminal offence of unlawful processing of personal data.

In that case the defendant was acquitted due to a state of necessity which removes the imputation (art.32 CC)

14

Dark web investigations
Case study

Videos and photos with child pornography on the darknet indicating that the perpetratror was a greek resident

Lawful interception of communications ordered by the judicial council and a house search followed,during which skype and google accounts were searched and the material found on the account files was printed.

Hard disks, laptops, mobile phones, SIM cards and micro sd cards were seized and sent to the Digital Forensic Department

In this case one of the mobile devices was protected by a code, which was not broken BUT

Lots of files found on hard discs as well as a browser providing access to darknet

15

Special investigative techniques Case study

A judicial council decision was issued permitting the interception of communications and the undercover police investigation in a file sharing application, where child pornography material was shared and a user (Greek resident) had a file with child pornography available for sharing

The undercover agent obtained the password of the file. The IP used and the subscriber data of the user were disclosed. A house search was conducted but no child pornography was found. However it was noticed that more than one PCs were connected to the router.

The e-mail used for the creation of the account was given to the authorities and the subscriber data of the owner of the account was disclosed. New house search but again no material relating to child pronography was found....

16

And the invstigation goes on...

A picture of the administrator of the account was shown to the resident of the last appartement searched, who recognised an old classmate living next door.

A new house search on the latter´s house where child pornography was found on the pc, as well as the communication with the undercover agent and the photo used for the creation of the account, which was taken by a NOKIA 500 mobile also found and seized in the appartment.

Hard disc and the mobile phone were sent to the Digital Forensic Department. The report drafted confirmed that the photo was taken by a NOKIA 500. According to the report pornography material, the file sharing and communication software and the account used for the dissemination of the material were stored in the hard disc.

17

Thank you

Questions?

18

Bavarian State Ministry of Justice

Obtaining e-Evidence when Investigating and Prosecuting Crimes

Thessaloniki, 16 February 2023 – 17 February 2023

Cross-border interception of telecommunication – legal challenges and solutions

With financial support from the European Union

1

Bavarian State Ministry of Justice

Structure of presentation

Cross-border interception of telecommunications

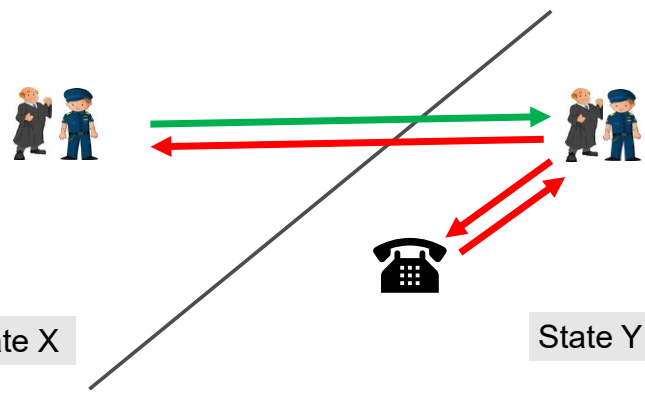
with/without

technical assistance of the target state

2

Bavarian State Ministry of Justice

Cross-border interception **with** technical assistance

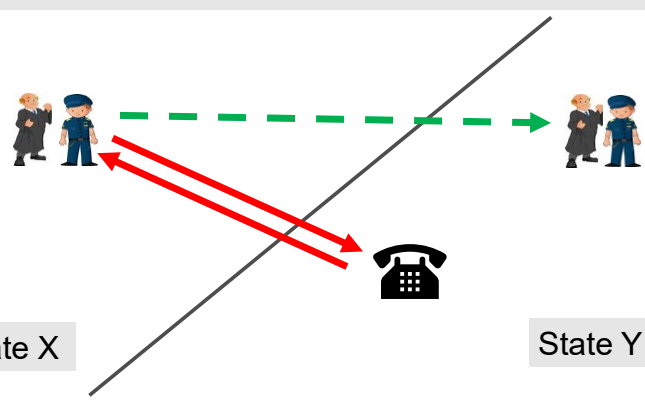


3

3

Bavarian State Ministry of Justice

Cross-border interception **without** technical assistance



4

4

Bavarian State Ministry of Justice

Cross-border interception **with** technical assistance: *Legal basis of cooperation*

- **Third States:**
  applicable multi-/bilateral MLAtreaties, e.g.:

  art. 34 Budapest Convention (EU+ USA, Canada, Australia, Brasil, Japan): obligation to assist with „real-time collection or recording of content data of specified communications transmitted by means of a computer system"

- **EU:**

  European Investigation Order (Directive 2014/41/EU)

5

5

Bavarian State Ministry of Justice

Cross-border interception **with** technical assistance: *EIO Directive*

- **Advantages** (principle of mutual recognition):
  - exhaustive catalogue of grounds for refusal
  - no double-criminality check
  - standardised forms
  - direct transmission to issuing state (art. 30 par. 6 (a) EIO Directive)
  - time limits (30+90 days)

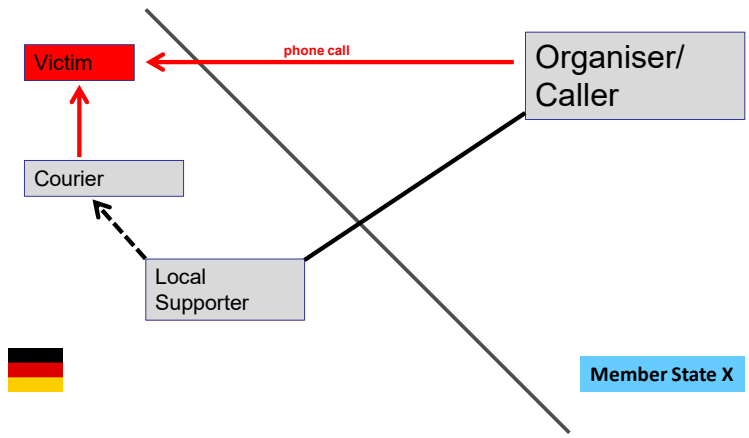
- **But:** art. 30 par. 5 EIO Directive:
  „execution of an EIO (…) may also be refused where the investigative measure would not have been authorised in a similar domestic case"

6

6

Bavarian State Ministry of Justice

Cross-border interception **with** technical assistance: *Case Example: Grandchildren trick*



7

7

Bavarian State Ministry of Justice

Levels of cross-border cooperation

8

8

Bavarian State Ministry of Justice

Cross-border interception **without** technical assistance: *Legal basis of cooperation*

- **Third States:** ???
- **EU:** art. 31 EIO Directive

  Concept:
  - target of interception is located in other MS
  - interception possible without assistance of that MS
  - ⇒ Obligation to notify that MS without undue delay
  - Notified MS can object within 96 hours

9

9

Bavarian State Ministry of Justice

Cross-border interception **without** technical assistance: *Case Example: Encrochat*

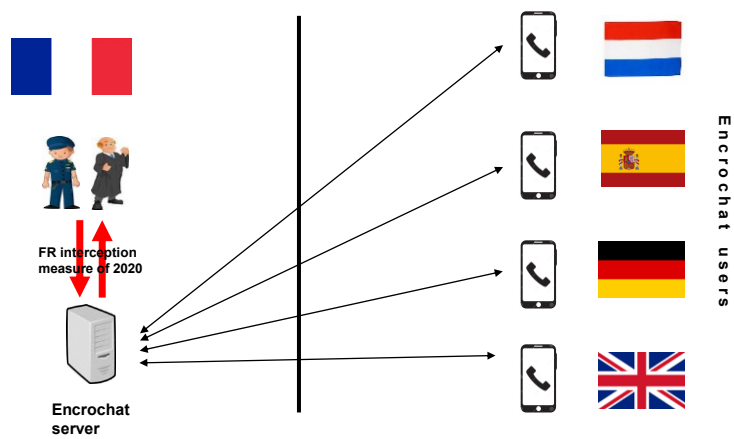
- FR investigation in 2018 re criminal organisation promoting and selling **„Encrochat" crypto-phones** for criminal use
- Indications for **criminal purpose** of crypto-phones, e.g.:
  - testimony of suspects in drug-trafficking investigations,
  - promotion of encryption technology and security features (e.g. „panic mode"),
  - high price,
  - impossibility to determine responsible entity
- Confirmed by **seizure of copy of FR Enrochat server** in 2019 and partial decryption of notes stored by Encrochat users

10

10

Bavarian State Ministry of Justice

Cross-border interception **without** technical assistance: *Case Example: Encrochat*



11

11

Bavarian State Ministry of Justice

Cross-border interception **without** technical assistance: *Case Example: Encrochat*

Cooperation between FR and DE authorities:

- **Direct contact** arranged via Eurojust
- **Spontaneous transfer of intercepted data** re DE users to BKA via Europol
- Initiation of **investigation** by GPPO Frankfurt against (unidentified) DE Encrochat users
- **EIO by GPPO Frankfurt** aiming at transfer of intercepted **data in the posession of FR authorities** re DE users
- **Authorisation by FR authorities to use transferred data** in DE court proceedings

12

12

Bavarian State Ministry of Justice

Cross-border interception **without** technical assistance: *Case Example: Encrochat*

Decision of Federal Court of Justice of 2 March 2022 (5 StR 457/21): transferred data is admissible as evidence in DE court proceedings

admissibility test: inadmissibilitiy only if

- violation of procedural law,
- that law protects the interests of the suspect and
- interest of suspect exceeds interest of prosecution

13

13

Bavarian State Ministry of Justice

Cross-border interception **without** technical assistance: *Case Example: Encrochat*

Decision of Federal Court of Justice of 2 March 2022 (5 StR 457/21): transferred data is admissible as evidence in DE court proceedings

analysis of possible violations of procedural law:

- FR law: legal basis for interception measure of 2020
  (only fundamental principles of the rule of law)
- art. 31 EIO Directive (obligation to notify target state)
- art. 6 par. 1 EIO Directive (necessity/proportionality of the EIO and possibility of requested measure under domestic law)

14

14

Bavarian State Ministry of Justice

Cross-border interception **without** technical assistance: *Case Example: Encrochat*

Regional Court of Berlin, request of 19 October 2022 for preliminary ruling by the ECJ (C-670/22):

EIO by GPPO Frankfurt

- is **disproportionate** (reference to ECJ decisions on data retention)
- violates art. 6 par. 1 b) EIO Directive, because **FR interception measure** has been conducted with the aim of an eventual prosecution in DE, although it **would not have been permissible under DE law**

15

15

Bavarian State Ministry of Justice

Thank you for the attention!

Michael Rothärmel
Email: michael.rothaermel@stmj.bayern.de

16

16

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

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

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

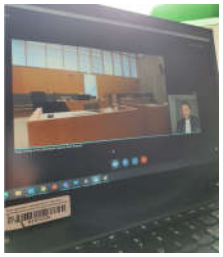
1

Introduction

Studies:
- Computer Science
- Law School

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

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



2

Guideline

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

3

We are under attack

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

Cybercriminals are increasing efficiency with coordinated attacks

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

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

4

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

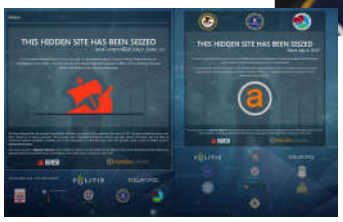
5

Developments

'Investeer in aanpak cybercrime'

Achievements

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



6

Mutual Legal Assistance

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

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

7

General Principles International Cooperation in Criminal Matters

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

8

Difficulties traditional MLA in cybercrime cases

Traditional legal concepts

Territoriality

Jurisdiction

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

9

European Production and Preservation Orders
Background

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

First

Digital evidence is held on servers owned by service providers.

Second

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

10

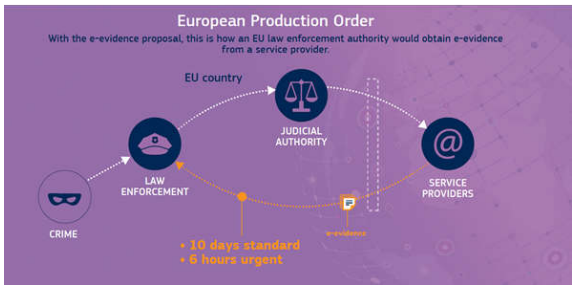
European Production and Preservation Orders
Summary of the proposed Regulation

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

11

European Production and Preservation Orders
Legal Basis, Subsidiarity and Proportionality

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



12

Status

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

13

European Production and Preservation Orders
Legal Basis, Subsidiarity and Proportionality

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

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

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

14

Innovation Law in the Netherlands

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

15

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

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

Synchronization? Existing connection?

16

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

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

Territoriality? Existing connection?

17

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

18

OSINT on Facebook: 'SlickRick'

19

OSINT on Facebook: 'SlickRick'

- OSINT on Facebook: 'SlickRick'
- Request subscriber data
  - Telephone number
  - IP address

20

Phone number / IP-address

21

Phone number / IP-address

- Phone number Bulgaria telecom provider. Sim only
- IP Address IP6V
- Last accessed by TOR

22

Chat Function:

- Undercover?
- Hacking?

23

Investigating the video and the victim's laptop:

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

24

Investigating the video and the victim's laptop:

- RAT → connecting?
- Whatsapp
- Password Vault?

25

Investigation:

- Investigating the Police systems
- Investigation Bitcoin account
- Cooperation at Europol
- Plot twist and final

26

16 February 2023

de Rechtspraak
Rechtbank Zeeland - West-Brabant

Thanks!

Questions?

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

27

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

THESSALONÌKI, 17 FEBRUARY 2023

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

With financial support from the European Union

ΕΣΔΙ
NATIONAL SCHOOL OF THE JUDICIARY

1

OUTLINE

I. Drawbacks of traditional Collection Mechanisms

II. The preference for direct cooperation between LEAs and Service Providers / Legal mechanisms enhancing this cooperation:

1. Direct transborder access (art. 32 Budapest Convention);
2. Production orders (art. 18 Budapest Convention);
3. *Ex cursus*: the U.S. Legal framework;
4. *De facto*: voluntary disclosure;
5. The II Protocol of the Budapest Convention

2

A COMMON DIRECTION….AND ITS REASONS

Enhancing public-private partnerships

Reasons:

1. the relevance of electronic evidence in criminal proceedings;

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

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

3

(THE COMPLEXITY OF) THE LEGAL FRAMEWORK

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

-the II Protocol of the Budapest Convention;

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

-Next steps:

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

4

COMMON PROBLEMS

1. Definitions
   - lack of a common definition for «electronic evidence»
   - the Budapest convention concepts: subscriber/traffic/content data
2. Actors
3. Data retention

5

ALTERNATIVES TO MLA

A. Direct Transborder Access;

B. Production orders to Service Providers;

C. Voluntary Disclosure or Public/private partnership

6

DIRECT TRANSBORDER ACCESS

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

- Art. 32 (b) Budapest Convention
  - "A Party may, without the authorisation of another Party… access or receive, through a computer system in its territory, **stored computer data located in another Party**, if the Party obtains the **lawful and voluntary consent** of the person who has the **lawful authority to disclose** the data to the Party through that computer system."

7

DIRECT TRANSBORDER ACCESS

Limits:

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

8

ART. 18 OF THE BUDAPEST CONVENTION

- A forerunner: direct „dialogue“ between LEA and SP
- : Article 18(1)(b) Budapest Convention

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

  b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control”
- Key points:
  - Subscriber information only
  - “offering its services in the territory of the Party”?
  - Data in the SP‘s possession or control (regardless of where the data is physically located)
- *Belgium v. Yahoo!* (Supreme Court of Belgium, 1 December 2015)

9

THE U.S. LEGAL FRAMEWORK

- How U.S. Authorities may access data located abroad (Microsoft Case/C.L.O.U.D. Act - The Clarifying Lawful Overseas Use of Data Act);
- How and to what extent U.S. Providers “share” data with foreign authorities;

10

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

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

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

- Motion to **quash or modify the order** (18 U.S.C. § 2703 (h) if:
  - the customer or subscriber is not a United States person and does not reside in the United States;
  - the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

11

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

- traffic data and subscriber information (voluntary disclosure; 18 U.S.C. § 2702, (c)6)
- When requested to do so, service providers are now allowed to disclose **content** data directly to "**qualifying foreign nations**", i.e. nations with whom the U.S. has signed an executive data sharing agreement (so-called CLOUD Act agreement) - § 2702 (b) (9) - 2703, 5

12

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

- Cloud Act Agreements: restrictions on type of government and type of information
- After the CLOUD Act
  - Neither the Act nor the agreements it authorizes create a legal obligation for service providers to comply with foreign governments' data demands
  - Concerns raised with respect to privacy, human rights and civil liberties

13

VOLUNTARY COOPERATION

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

Pros: it can be fast and effective

Cons:

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

14

HURDLES AND TOOLS

-Legal/Procedural hurdles

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

Tools: policies, guidelines, templates for requests - SIRIUS

The perspective of the service provider: costs

15

THE SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION

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

2. enhancement of MLA instruments (Section 3 – Procedures enhancing international co-operation between authorities for the disclosure of stored computer data)

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

4. Safeguards (art. 14)

16

SECTION 2 – ENHANCING DIRECT COOPERATION WITH PROVIDERS

Art. 6 – Request for domain name registration information

Art. 7 – Disclosure of subscriber information

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

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

17

SECTION 2 – ENHANCING DIRECT COOPERATION WITH PROVIDERS

What kind of data ?

- -domain names
- -subscriber information

What kind of private entity?

- Registrars
- Service providers

Enforcement

18

SECTION 3 – ENHANCING INTERNATIONAL COOPERATION BETWEEN AUTHORITIES

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

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

a. **subscriber information**, and

b. **traffic data**

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

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

19

SECTION 3 – ENHANCING INTERNATIONAL COOPERATION BETWEEN AUTHORITIES

Key issues:

-purpose;

-scope;

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

-time.

20

ART. 9 AND 10 – EMERGENCY DISCLOSURE

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

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

Scope:

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

21

THANK YOU FOR YOUR ATTENTION!

22

1

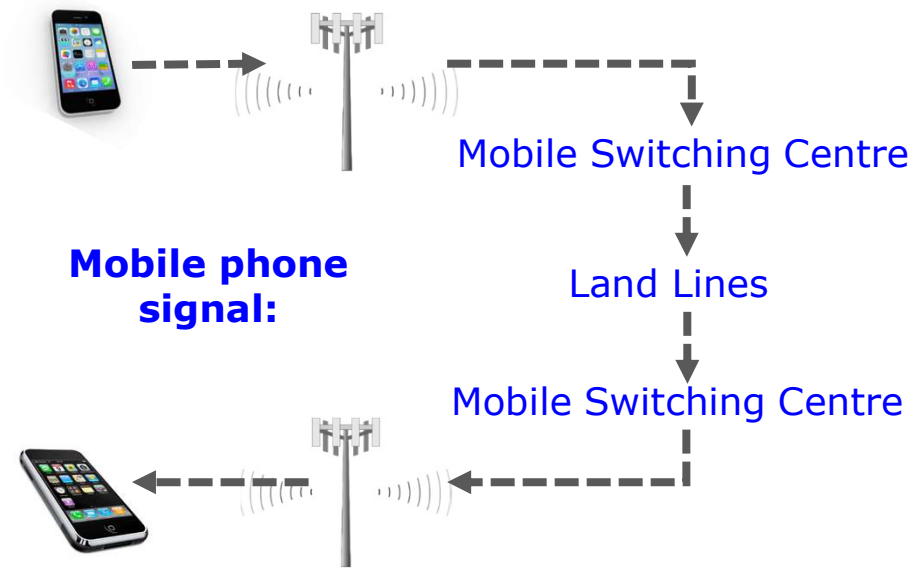
Two (main) mobile phone systems:

- GSM (Global System for Mobile Technology)
- CDMA (Code Division Multiple Access) – mainly USA

Telecoms companies share their networks (= 'roaming')

InZeit

2



3

Phones

Identifiers:

SIM (Subscriber Identity Module) Card

IMEI/IMSI Numbers
International Mobile Equipment Identity
International Mobile Subscriber Identity

(Most phones display the IMEI when you key in ***#06#**)

Subscriber Account details

4

SIM Card

Authorises phone number on a telecoms network.

May contain
- call history
- contacts and
- received texts

SIM can be switched between different phones

Some modern SIM cards have Secure Element that stores credit card details to allow use as payment device

InZeit

5

Different 'generations' 1G – 5G

1st Generation – Analogue Radio Waves

2nd Generation (2G) since early 90s Calls + texts (64 kilobits per second)

3G calls + text + Internet + video

4G High quality applications
(1 Gigabit (billion) per second)

5G ('launched' end 2018)

InZeit

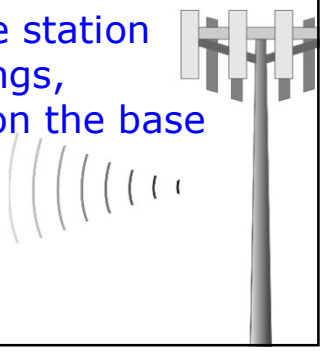
6

When phone switched on sends a signal ('ping') to the network.

It selects the most powerful base station

Registered on system (if phone on standby will 'ping' periodically)

Not necessarily the closest base station (affected by topography, buildings, weather, reflected signal, load on the base station)



InZeit

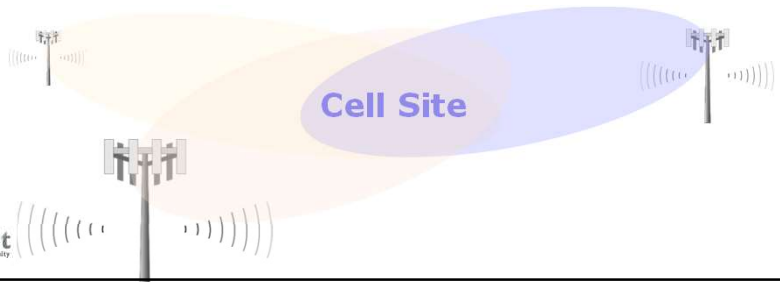
7

During a call, the network will control to which tower the phone is connected.

When crosses cell site boundary the phone is 'handed off' to the next tower.

Each 'dish' on a cell site antenna has an identifying number.

The antenna number is recorded.



InZeit

8

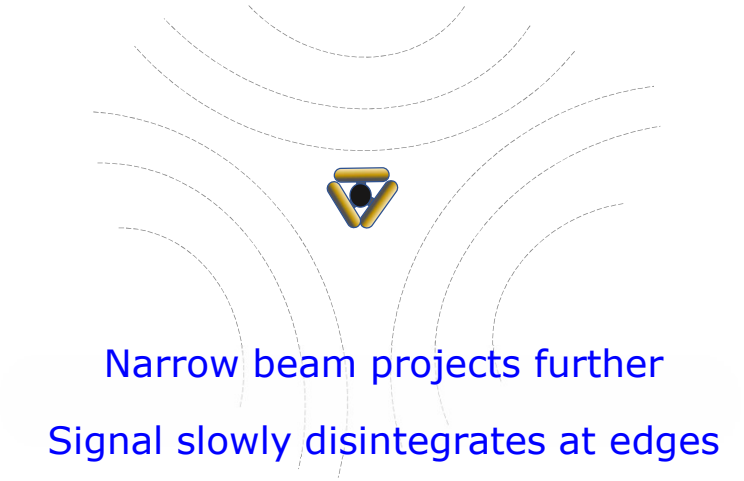
Cell Site Analysis

- Historical cell site & call data analysis
  - Which cell tower used
  - Number called
  - Time and duration of call
  - IMEI (physical number on phone)
  - IMSI (identifying the user account)
- Transaction records for billing
- Can be 'near' real time
- Even site surveys can't reproduce all variables

InZeit Excellence in Acuity

9

Depending on number of dishes, one dish may cover 60° - 180° (here 120° sector shown)

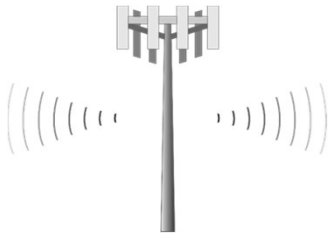


Narrow beam projects further

Signal slowly disintegrates at edges

InZeit Excellence in Acuity

10



Urban area: single tower can identify phone location to within an area of about 1km^2

Rural setting may be 10s of km^2

Note: Cell-site sectors are not neat shapes with clearly defined edges (diagrams can be misleading)

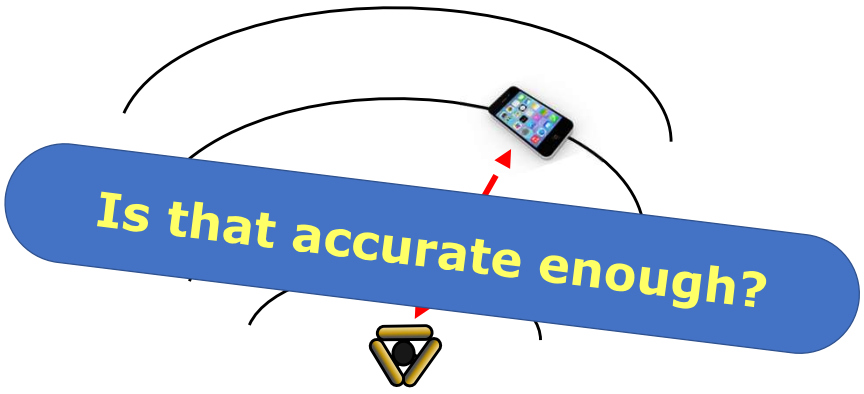
Cell-site sectors overlap

4G phones may connect to more than 1 cell-site

InZeit

11

Time difference of arrival (TDOA)



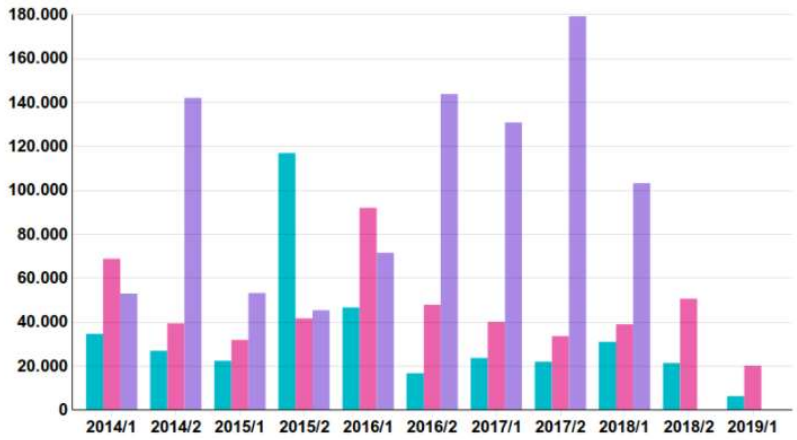
Can *estimate* phone distance from antenna from time signal takes (pinging)

InZeit

12

Stealth (sms) Ping

Causes phone to register on (nearest) mast



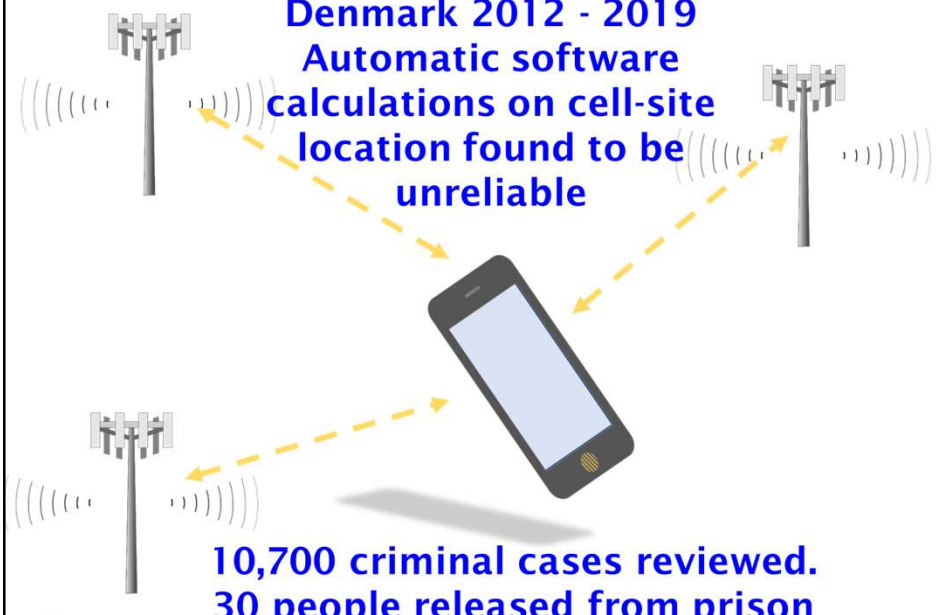
BKA Federal Criminal Police
BPOL Federal Police
BfV Federal Office for the Protection of the Constitution

InZeit

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

13

Denmark 2012 - 2019
Automatic software calculations on cell-site location found to be unreliable



10,700 criminal cases reviewed.
30 people released from prison

InZeit

14

In 2004 Lisa Roberts pleaded guilty to manslaughter on a plea bargain on advice of her (court appointed) attorney

Prosecutor had told the attorney that phone records put Roberts at the scene and was 'almost as accurate as DNA'.

InZeit Excellence in Acuity

https://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html?utm_term=.e1ea86444ad2

15

2014 (9 ½ years imprisonment) Lisa Marie Roberts released. Cell-site analysis was found to be inaccurate.

InZeit Excellence in Acuity

https://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html?utm_term=.e1ea86444ad2

16

GPS

17

Global Positioning System (GPS)

Handsets have GPS chip

Network of 30+ satellites 27,000 km orbit. Always 6 'in view'

Requires clear view of min. three (better four) satellites

Where no satellite connection, phone may use wifi or phone network

On average, location identifiable to 5-8 metres (can be 3-5 metres – future tech 30cm)

18

Geofence Warrants & Google's Sensorvault

Who has an Android phone?

72.32% Android Global Market Share
(Dec 2022)
https://techjury.net/blog/android-market-share/

Location data saved to 'Sensorvault' database

19

Sensorvault

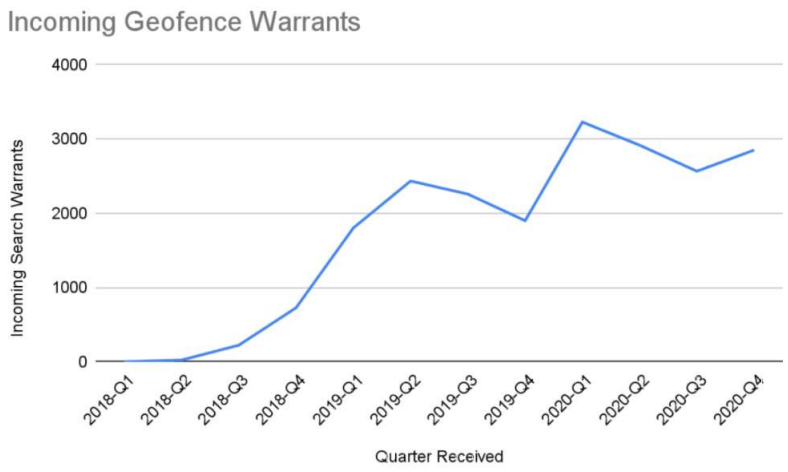
Google's Sensorvault database contains location data for hundreds of millions of devices all over the world.

Law enforcement officials use 'Geofence warrants' to obtain information from Sensorvault to identify suspects in vicinity of a crime.

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

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

20



25% of all US warrants received by Google in 2020

InZeit

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

21

Milwaukee, Wisconsin, USA June 2017

Middle of the night - Woman car jacked by 2 males

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

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

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

InZeit

22

Geofence Warrant sought & obtained within 12 hours

Forwarded to Google flagged "exigent circumstances"

20 minutes later Google called back

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

InZeit

23

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

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

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

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

5 Days from crime report to arrest – DIFFERENT STATES.

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

24

InZeit

Milwaukee to Louisville 400 miles (650km)

25

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

[Can be combined with 'Keyword Warrant' – both Geofence and Keyword Warrants under attack in the USA as 'unconstitutional']

InZeit

26

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

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

27

Is the assumption of accuracy and integrity of technology good enough?

'Machine Testimony' Andrea Roth
126 Yale L.J. (2017)

'Wayne Dobson doesn't have your cellphone.'

https://www.reviewjournal.com/local/local-las-vegas/if-you-lose-your-cellphone-dont-blame-wayne-dobson/

GPS data can be hacked and altered in real time

https://www.wired.com/2015/07/hackers-heist-semis-exploiting-satellite-flaw/

28

Location Based Services

- SatNav Driving instructions
- Uber taxi app
- Nearby restaurants
- Where car parked

29

Location-as-a-Service

Location as a service (LaaS) is a location data delivery model where privacy protected physical location data acquired through multiple sources including carriers, Wi-Fi, IP addresses and landlines is available to enterprise customers through a simple Application Programming Interface (Wikipedia)

30

Your location traded commercially with your 'consent'

Thinknear suggests 54% of reported Location Based Service locations are out by more than 1000 metres.

https://computing.derby.ac.uk/c/accuracy-of-location-services-on-smart-devices/

InZeit

31

SECURUS TECHNOLOGIES

In USA Securus Technologies is contracted to provide & monitor prison phone calls.

Location service 'able to find any AT&T, Sprint, T-Mobile or Verizon phone in USA' using data supplied through company called Locationsmart.

Data legitimately used for search & rescue finding lost/missing persons or fugitives.

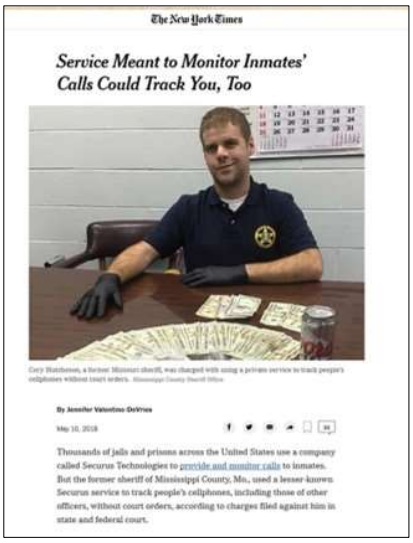
The information is 'volunteered' by phone users through phone contract terms.

InZeit

32

(According to press reports)

2014-2017 Sheriff Cory Hutcheson of Mississippi County, Missouri, USA obtained 100s of phone locations from Securus Technologies without authorisation.



The New York Times

Service Meant to Monitor Inmates' Calls Could Track You, Too

By Jennifer Valentino-DeVries

May 10, 2018

Thousands of jails and prisons across the United States use a company called Securus Technologies to provide and monitor calls to inmates. But the former sheriff of Mississippi County, Mo., used a lesser-known Securus service to track people's cellphones, including those of other officers, without court orders, according to charges filed against him in state and federal court.

https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html

InZeit Excellence in Acuity

33

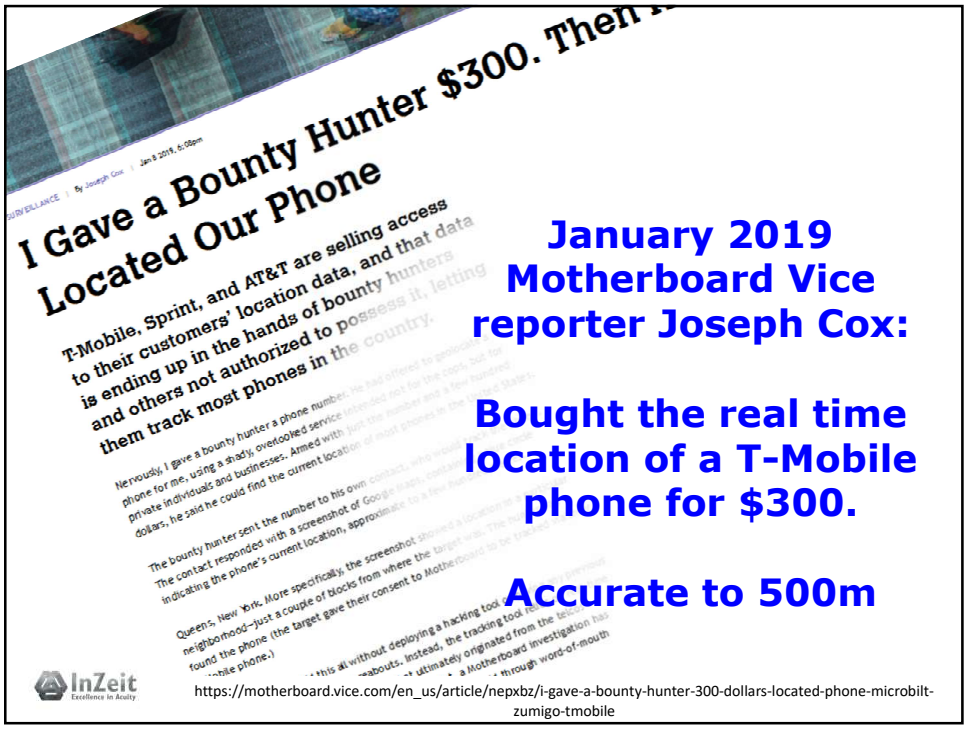
Nov 2018 (ex-)Sheriff Hutcheson pleaded guilty to federal wire fraud charges and to illegally possessing and transferring the means of identification of others

29th April 2019 Sentenced to 6 months Federal prison

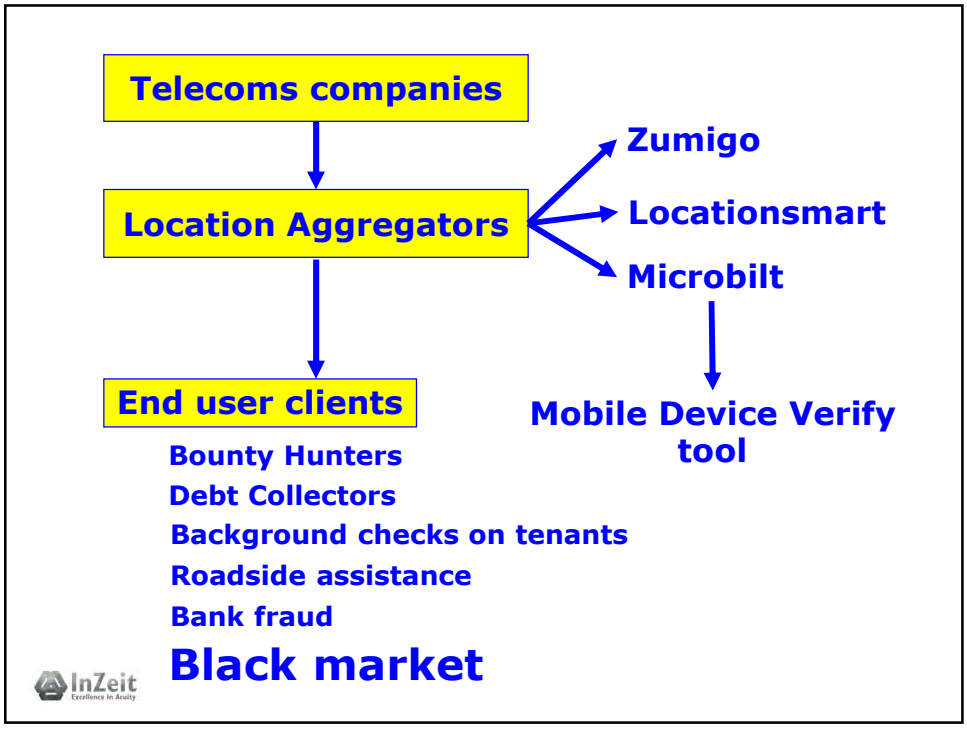
https://www.ky3.com/content/news/Ex-Missouri-sheriff-sentenced-to-6-months-in-fed-prison-509223001.html

InZeit Excellence in Acuity

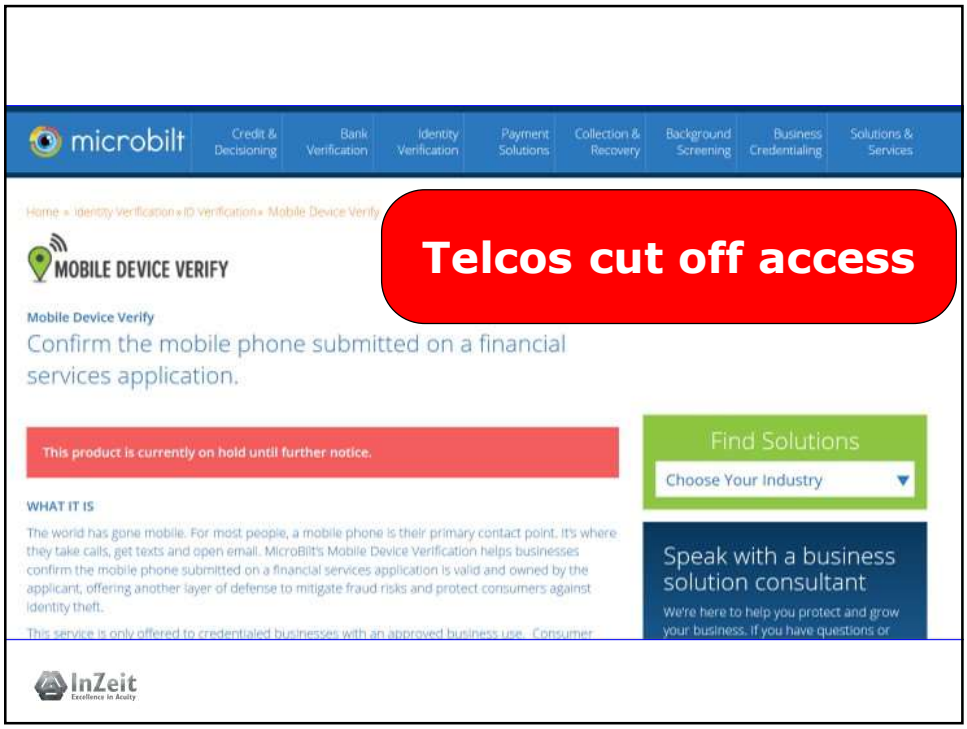
34


I Gave a Bounty Hunter $300. Then I Located Our Phone
T-Mobile, Sprint, and AT&T are selling access to their customers' location data, and that data is ending up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country.
January 2019 Motherboard Vice reporter Joseph Cox:
Bought the real time location of a T-Mobile phone for $300.
Accurate to 500m
https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

35


Telecoms companies
Location Aggregators
Zumigo
Locationsmart
Microbilt
End user clients
Mobile Device Verify tool
Bounty Hunters
Debt Collectors
Background checks on tenants
Roadside assistance
Bank fraud
Black market

36



37

IMSI Catcher
(aka StingRay, Hailstorm, TriggerFish)

Device imitates mobile phone base station

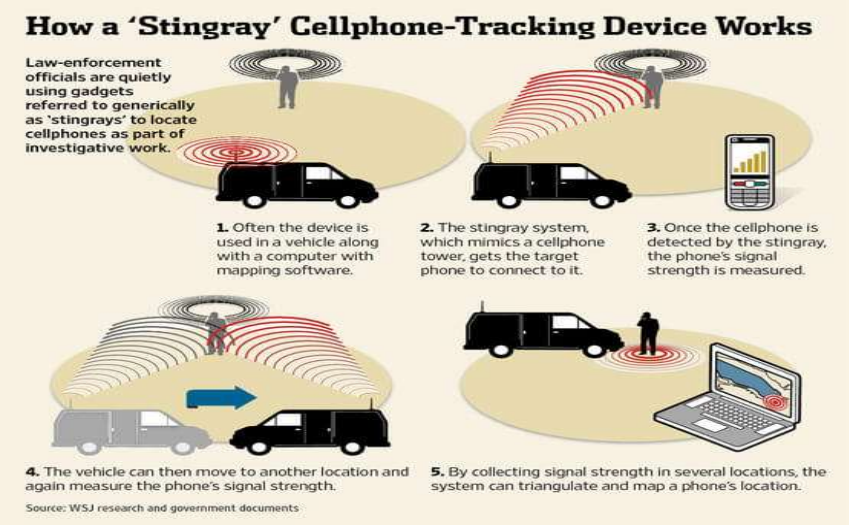
Phone automatically detects & connects to the IMSI catcher

All phone traffic passes through the IMSI catcher

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

InZeit

38



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

InZeit

39

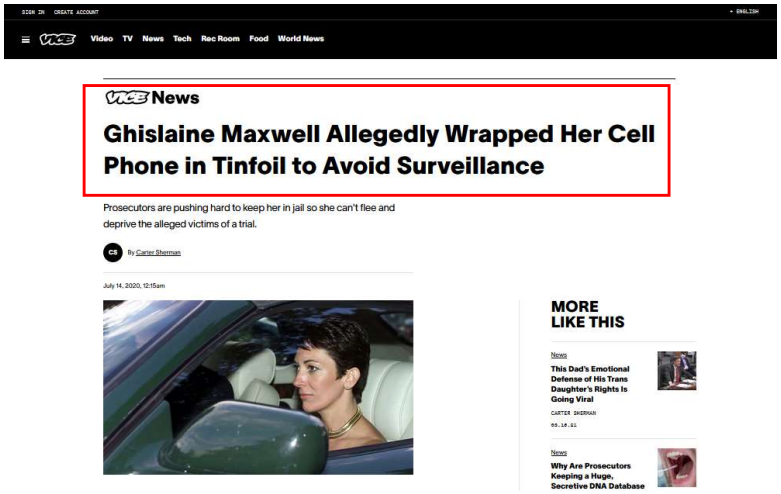
If phone powered off or isolated (e.g. inside a Faraday bag), it cannot be located.

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

InZeit

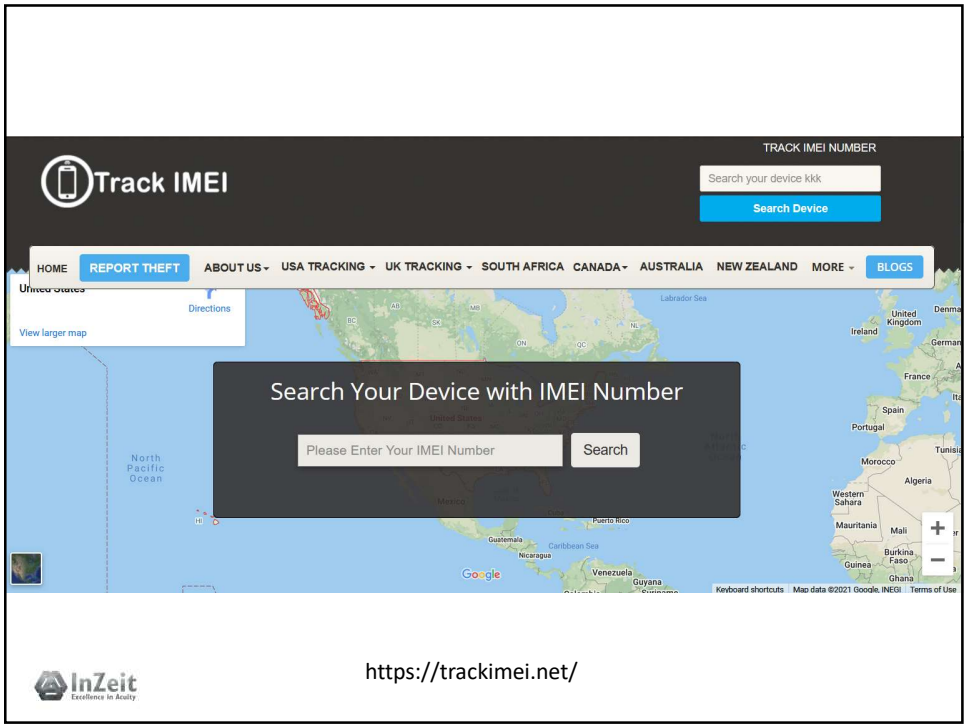
40

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



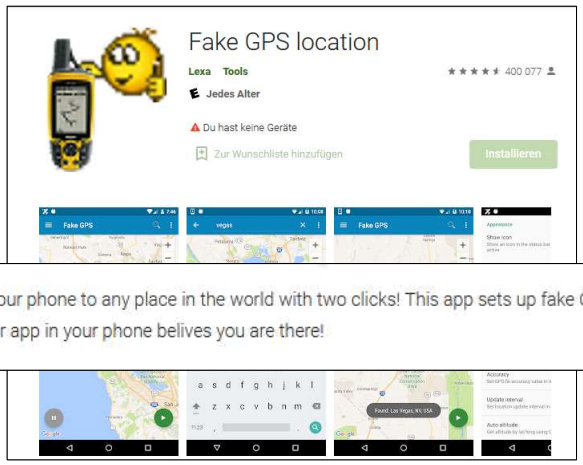
'Cell phone data' (GPS and/or cell site analysis) > 1 square mile (2.59 km^2)

41

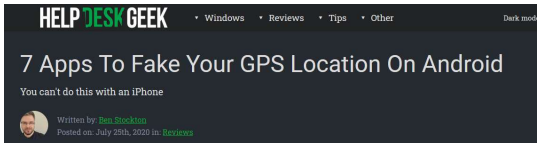


https://trackimei.net/

42



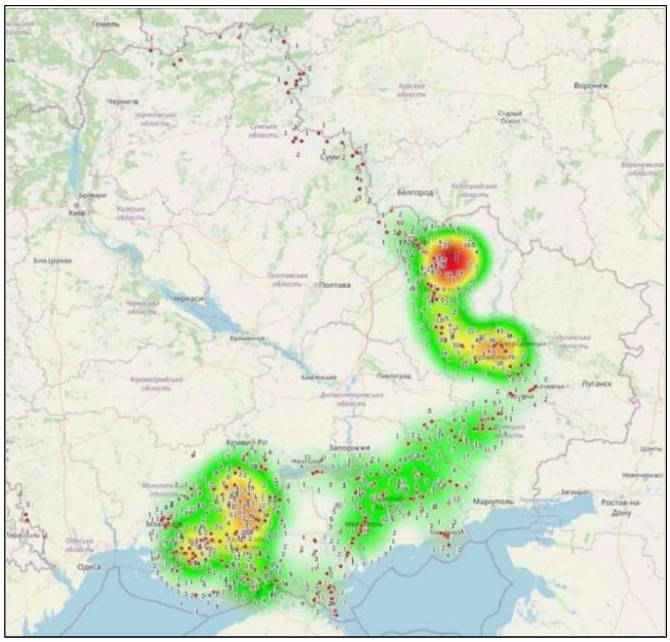
https://play.google.com/store/apps/details?id=com.lexa.fakegps&hl=de_AT&gl=US



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

43

Active Russian SIM cards (May 2022)



Source: Linkedin Post by Dan Kaine, Inherent Risks

44

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

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

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

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

InZeit

45

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

- **EXCLUSIVE: Kremlin has compiled a database of mobile phone numbers**
- **The information was gathered by spies near some of the UK's most sensitive**

Moscow blames its troops' use of mobile phones for Makiivka missile strike

Ukrainian shelling that killed 89 recruits aided by mobiles switched on near frontlines, claims Russia defence ministry

https://www.theguardian.com/world/2023/jan/04/moscow-blames-its-troops-use-of-mobile-phones-for-makiivka-missile-strike

InZeit

46

Summary

Identifiers: SIM, IMEI, Subscriber details

Cell-Site Analysis influenced by lots of factors (technical/topographical/meteorological)

Ways of tracking phone include: Cell-Site Analysis, GPS, IMSI Catchers, Sensorvault, Silent ping, Location-based services

Signal can be easily hidden or spoofed

InZeit

47

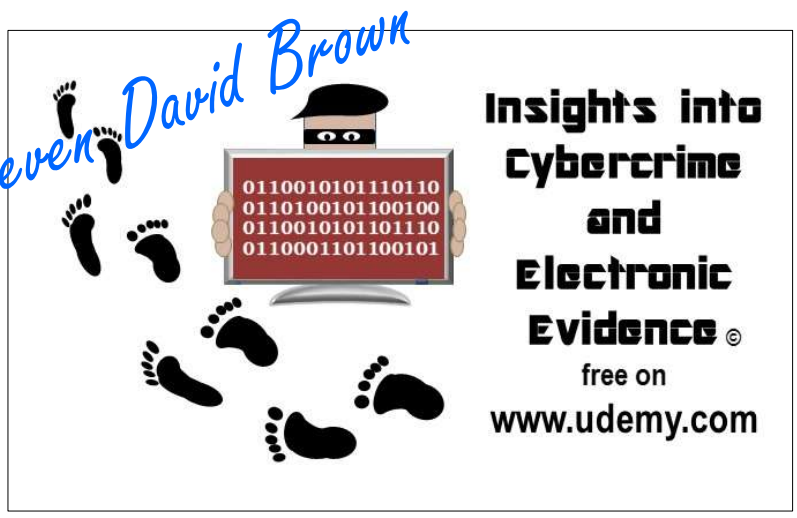
info(at)inzeit(dot)eu

InZeit

48

Some Reference Material

49



https://www.udemy.com/insights-into-cybercrime-and-electronic-evidence/

50

Barratt, B. (2018) A Location-Sharing Disaster Shows How Exposed You Really Are https://www.wired.com/story/locationsmart-securus-location-data-privacy/

Berkeley Law (2015)"Cell Site Simulator Primer" https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-4-28_Cell-Site-Simulator-Primer_Final.pdf

Cox, J. (2019) *I Gave a Bounty Hunter $300. Then He Located Our Phone* https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

Daniel. L (2019) *Cell phone location evidence for Legal Professionals* Academic Press

Hollister, S. (201) Carriers can sell your location to bounty hunters because ISP privacy is broken https://www.theverge.com/2019/1/8/18174024/att-sprint-t-mobile-scandal-phone-location-tracking-black-market-bounty-hunters-privacy-securus

Krebs, K. (2018) *Tracking Firm LocationSmart Leaked Location Data for Customers of All Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site* https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/

Krebs, K. (2021) *Can We Stop Pretending SMS Is Secure* Now? https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/

Nicol, M. (2022) *Russian Spies Tracking British Former Special Forces Teams by their mobile numbers* https://www.dailymail.co.uk/news/article-10629125/Russian-spies-tracking-British-former-special-forces-teams-mobile-numbers.html

51

Monroy, M. (2019) Less „Silent SMS" from German police, but more secrecy for domestic Intelligence https://digit.site36.net/tag/silent-sms/

Sauer, P. (2023) *Moscow blames its troops' use of mobile phones for Makiivka missile strike https://www.theguardian.com/world/2023/jan/04/moscow-blames-its-troops-use-of-mobile-phones-for-makiivka-missile-strike*

Schuppe, J. (2020) *Google tracked his bike ride past a burglarized home. That made him a suspect.* https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761

U of Derby DECM (2019) *Accuracy of Location Services on Smart Devices* Blog https://computing.derby.ac.uk/c/accuracy-of-location-services-on-smart-devices/

Valentino-DeVries, J. (2019) *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works* New York Times (13/04/2013)

Valentino-DeVries, J. (2018) Service Meant to Monitor Inmates' Calls Could Track You, Too New York Times (10/05/2018)

Whittaker, Z (2019) *Despite promises to stop, US cell carriers are still selling your real-time phone location data* https://techcrunch.com/2019/01/09/us-cell-carriers-still-selling-your-location-data/

Kim Zetter (2015) *Hackers Could Heist Semis by Exploiting This Satellite Flaw* https://www.wired.com/2015/07/hackers-heist-semis-exploiting-satellite-flaw/

52

Mobile Phone Fake GPS Apps [Use at your own risk!]

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

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

Technical Insights, ACPO & The Digital Forensic Process

Timothy De Groot, Belgian Federal Police

With financial support from the European Union

1

Possible Devices

- Computer, laptop
- Mobile devices (wearables, drones, etc.)
- External devices (USB, memory card, etc.)
- Network devices (routers, switches, etc.)
- Cloud
- Gaming consoles
- In-Vehicle systems (GPS devices, navigation systems)
- IoT devices (smart home, home appliances, etc.)
- Digital video recording systems
- …

2

ACPO Principle

3

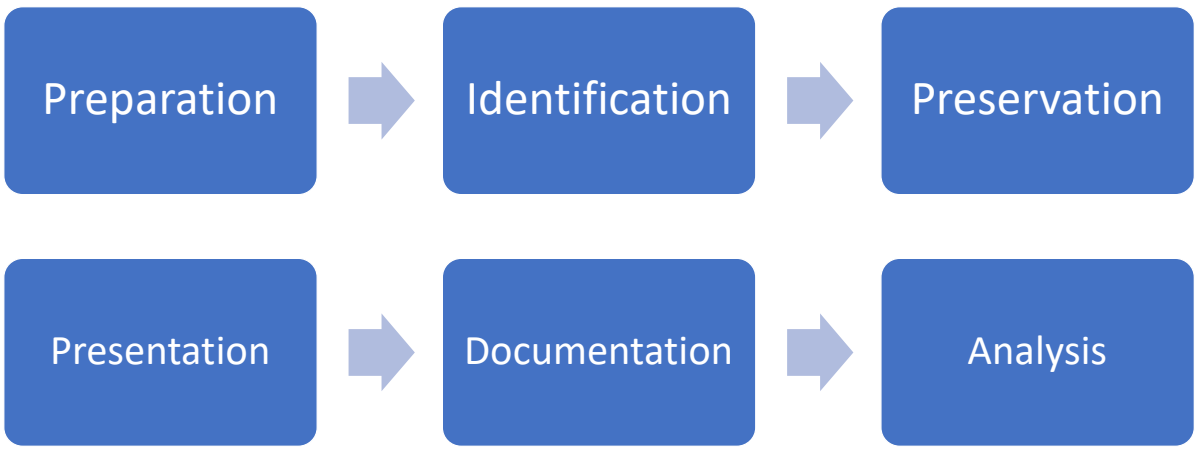
- "**No action** taken by law enforcement agencies, or their **agents should change data** held on a computer or storage media which may subsequently be relied upon in court"
- "In circumstances where a person finds **it necessary to access original data** held on a computer or on storage media, that **person must be competent** to do so and be able to give evidence **explaining** the **relevance** and the **implications** of their actions"

4

- "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 achieve the same result"
- "The **person in charge** of the investigation (the case officer) has **overall responsibility** for ensuring that the law and these principles are adhered to"

5

Principles



6

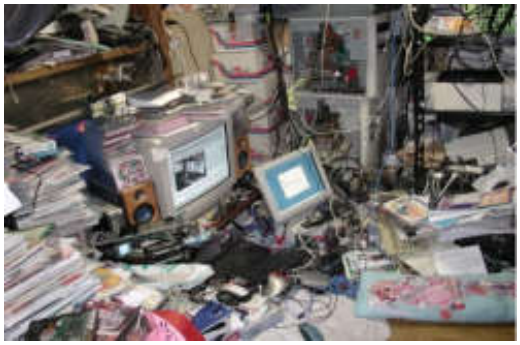
Preparation

- Purpose of investigation?
- What digital evidence do you expect to find?
- Home or office? – Administrator?
- Is there a network?
- Cloud storage utilized?
- Search Warrant?

7

Identification

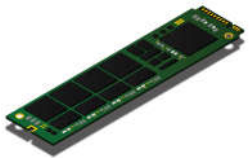
- The act of searching
- **Detecting** & **documenting** (digital) evidence
- DEFR must examine all devices used in the action of crime



8

Storage

- Storage media
- HDD
- SSD
- CD
- DVD
- USB
- …



9

Preservation

- Bag & Tag
- Transport
- Lab environment
- In-lab preservation

10

Chain Of Custody

- **Chronological** documentation of electronic evidence
- Indicates
  - the **collection**
  - **sequence** of control
  - **transfer**
  - **analysis**
- Includes documentation of:
  - Each **person** who **handled** the evidence
  - The **date/time** evidence was **collected** or **transferred**
  - The **purpose** of the transfer
- Preserving the **integrity** of the evidence and **prevent** it from **contamination**

11

Integrity Demo

12

Analysis

- **Analysis** and **examination** of electronically stored information
  Purpose: identify information that may support, or contest matters in a civil or criminal investigation and/or court proceeding
- Evidence should first be **extracted** or **acquired**
- Analysis should be performed on a **copy** of the **media**
- Tools used must be previously validated

13

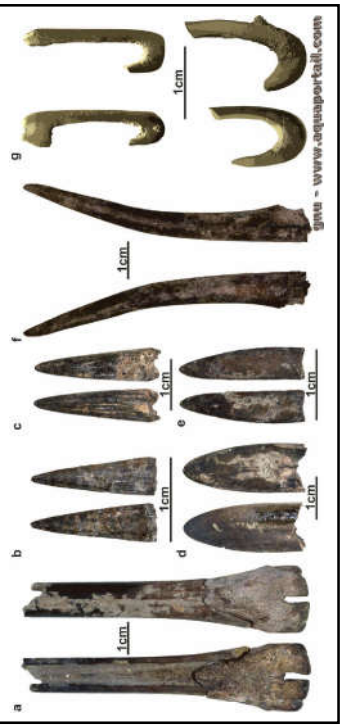
Operating System & File system

- Operating systems
  - Windows: vista, 7, 8, 10, 11 (and older)
  - macOS (changed names): Mojave, Catalina, Big Sur, Monterey (and older)
  - Linux & distro's: Debian, Ubuntu, Linux Mint, …
- File systems
  - NTFS, FAT32, exFAT, ReFS, …
  - HFS, HFS+, APFS, …
  - Ext3, Ext4, …

14

Intro to Forensic Techniques

- Artefacts
  - Browser history
  - Event logs
  - Registry
  - … (much more)
- File recovery
- Carving
- E-mail investigation (headers, pst, …)
- Network investigation
- Specific searches (Regular Expressions = filters)
- LDF
- …



15

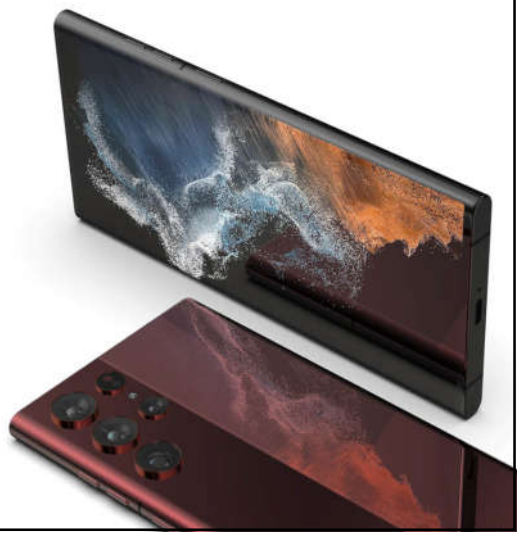
Analysis Demo

16

Mobile device for example

What can be found?

- Contacts Call **logs**
- Calendar
- Messages
- Emails
- Photographs
- videos
- Social networking **accounts**
- Notes
- documents
- **Financial** information
- Wi-Fi connections
- Internet browser **history**
- Applications
- Geolocations
- …



17

Documentation

18

Presentation

- **Everything** from digital evidence seizure to the end of analysis phase must be **explained**
- An investigator must be able to **state** that the **results** provided are **correct** and **weren't changed** in any way

19

Dead Box Analysis vs Live Data Forensics

20

SMALL CASE STUDY: Live Scene

What to do when encountering a booted computer at the crime scene?

21

Forensic Difficulties

- Closed hardware
- Password & 2FA
- Encryption
- Big volumes
- Time
- Hashing countermeasures
- Anti-forensic software
- Steganography
- Hidden volumes
- …

22

Questions & contact

Timothy De Groot

- **Mail:** timothy.degroot@police.belgium.eu
- **Tel:** +32 (0) 495 43 48 45
- **LinkedIn:** Timothy D.G.

23

Obtaining e-evidence in criminal investigation & prosecution
Special Investigation Techniques on mobile devices
Thessaloniki, 16- 17 February 2022

- E-EVIDENCE
  in child sexual abuse cases
- Investigation and prosecution of "everyday crimes"
- Greek jurisprudence
- Case studies

Speaker : Eleni Papadopoulou

Public Prosecutor at the Court of First Instance of Athens

With financial support from the European Union

ΕΣΔΙ
NATIONAL SCHOOL OF THE JUDICIARY

1

"Conventional" versus cyber-related abuse
Child sexual abuse crimes before and after the digital age

- Distinction
- A short overview of the most common child sexual abuse crimes before the rise of internet/digital crimes
- Focus on the challenges of investigating and prosecuting both "conventional" and cyber-related child sexual abuse crimes with a special interest in the most common of all cyber-related crimes: Child Pornography
- Getting e-evidence right; grounds for using it along with physical evidence which was the norm in the past
- E-evidence for "routine" crimes

2

Can e-evidence help the investigation ?

- Crime recordings
- Communication between the offender and the victim
- Mobile phones : An ally when the perpetrator is someone close to home…
- Areios Pagos 2081/2018: Text messaging revealed that the offender knew that the rape victim was a minor
- Testimonies versus text messaging : Adolescents like to talk with friends; not with experts
- Location data → the scene of the crime

3

Can e – evidence help the offender?

- Areios Pagos 101/2021: The disclosure of the encrypted code by the accused is not a mitigating factor at sentencing
- Is there an obligation for third parties to technically help the investigation?
- Article 18 of the Convention on Cybercrime : Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order : a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer – data storage medium; and b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control

4

"New" forms of Child Sexual Abuse Crimes → Cyber crimes

- Why is their investigation and prosecution more challenging?

One can distribute child pornography material from their home in Athens with a simple device

Swiftly

Anonymously

With Just a Click

In Texas …

5

Suspect identified; now what?

- HOUSE SEARCH - An essential and conventional investigation method
- COLLECTION – EXAMINATION – ANALYSIS – REPORT
  - Protect the scene: Find all mobile devices and ensure that no one has access to them
  - Record the time of the search, take photographs and keep a log
  - Check the devices- do they function properly?
  - Are there any devices remotely accessed by other devices?
  - Is data being destroyed?
  - Are there any indications of communication via Instant Messaging or Chat?
  - Collect/ collate additional physical evidence (such as codes on notes and manuals)

6

Suspect identified – additional actions

- "Live" digital forensics
- Phonebooks
- Open applications
- Confiscation of digital data especially data contained in a remote computer system
- Chain of custody
- Recover, store and guard all useful digital data
- Organise and analyse the data
- Copy and encryption
- Preparation of a comprehensive report → admissible in court. Areios Pagos 1033/2014 : The report regarding the technical analysis of a hard drive and the digital files are not documents but crime items.

7

Profile the suspect

Mobile devices → Analysis of the IE history file → How many hits on child pornography-related websites? Are there any anagrams? → Establishment of the crime or aggravating factor

Areios Pagos 643/2020, 1301/2019, 2081/2018, 1807/2018, 1133/2018: Possession and acquisition of pornographic material of children under 15 years old is not a felony if there isn't any processing, management, use, distribution or dissemination or other actions that entail the risk of dissemination and transmission of child pornography material.

8

Judicial Council of First Instance of Athens 1860/2019

- Europol received information regarding child pornography from the National Center for Missing and Exploited Children
- 2 IP addresses were traced in Greece
- The Cyber Crime Division was informed
- Request of a court order
- Identification of the suspect→ a woman?
- House search → confiscation of a lap top belonging to the husband
- Analysis → Two files containing child pornography material at the unallocated space → The husband was the suspect after all!

9

Claims of the accused

- Only 2 pictures in the laptop
- At the unallocated space
- Lack of IT knowledge
- Downloading video games containing links to webpages with chatrooms relating to child pornography WITHOUT his knowledge

10

Prosecutor's response

- 2 pictures equals 0 pictures? What sort of math is this?
- Unallocated space or not STILL in his possession!
- Shift of burden of proof → It was he who had to prove that he lacked the knowledge to retrieve the pictures from the unallocated space
- Experienced user : 1) downloading TOR, the Cc cleaner, 3) the Fileshredder
- Other arguments: Stepdaddy???? Really?

The accused was indicted before the Mixed Jury Court of First Instance of Athens. He has not yet been tried.

11

Another case… What did the search/investigation show?

- A hard drive was confiscated.
- A visual check of the suspect's laptop showed that the program ManyCam was downloaded.
- IE history check: the suspect was banned from the website Omegle due to inappropriate behavior.
- However, on 16-3-2016 he was able to obtain access to child pornography on this website.
- On the file "Downloads", there were one video and three pictures containing child pornography material.
- The hard drive of the suspect contained 5 videos of child pornography.

12

What did the accused claim?

- Chat on Omegle with unknown users who sent him hyperlinks
- The files were downloaded automatically without his knowledge.
  - A very common argument of the accused persons
  - Areios Pagos 643/2020 : The existence of other files essential to the accused' s profession in the same drive prove that he had knowledge of the child pornography material
- Poor IT knowledge

13

Judicial Council of First Instance of Nafplio 430/2021

- Poor IT knowledge? It was a fact that he did install ManyCam and used it to watch a child pornography video.
- He had access to DEEPWEB.
- He used signals and symbols with child pornography connotations to get access to such material.
- He visited OMEGLE many times until 2-3-2017 when he was banned from the site.

Indictment of the accused before the Mixed Jury Court of First Instance of Corinth

- He was found guilty
- He was sentenced to 4 years of imprisonment
- The hard disc containing child pornography material was SEIZED.

14

To summarise

Information → IP addresses → Police → Digital Traces → Prosecutor + Judicial Council → Court orders → Identification → House search → Seizure of Mobile devices + Visual check of the devices in real time → Forensic Analysis → Files containing pictures and videos + IE history + Downloading of programs useful to gain access to child pornography + Keywords with child pornography connotations = PROSECUTION and CONDEMNATION

Digital information used for the investigation consisted of IP addresses and digital traces, which was critical for the court orders and the subsequent identification of the suspect. The visual check of the devices (in real time) that were seized in the house search led to a forensic analysis which revealed a range of information including files with videos/pictures, IE history, keywords with child pornography as well as programmes download which was useful to gain access to child pornography =PROSECUTION & CONDEMNATION

15

Thank you for your attention!

Any questions or comments?

16