ERA
european.law

# OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

SPECIAL INVESTIGATION TECHNIQUES FOR MOBILE PHONES

Thessaloniki, 7-8 February 2022

UP GRADE
YOUR LEGAL EXPERTISE

Criminal Law

Professional Training (CPD)
www.era.int

## Speakers

**Steven David Brown,** International Cybercrime Consultant, Vienna

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

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

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

**Sapfo Katsanaki,** Prosecutor, Prosecutor's Office, Athens

**Eneli Laurits,** District Prosecutor, Department for Juvenile Crimes, Estonian Prosecutor's Office, Tallinn

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

**Danijel Sladović,** Digital Forensics Consultant, INsig2, Zagreb

**Remco Sprooten,** Senior Security Consultant, Teamleader, Security Operation Center, ENGIE NL, Amsterdam

## 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

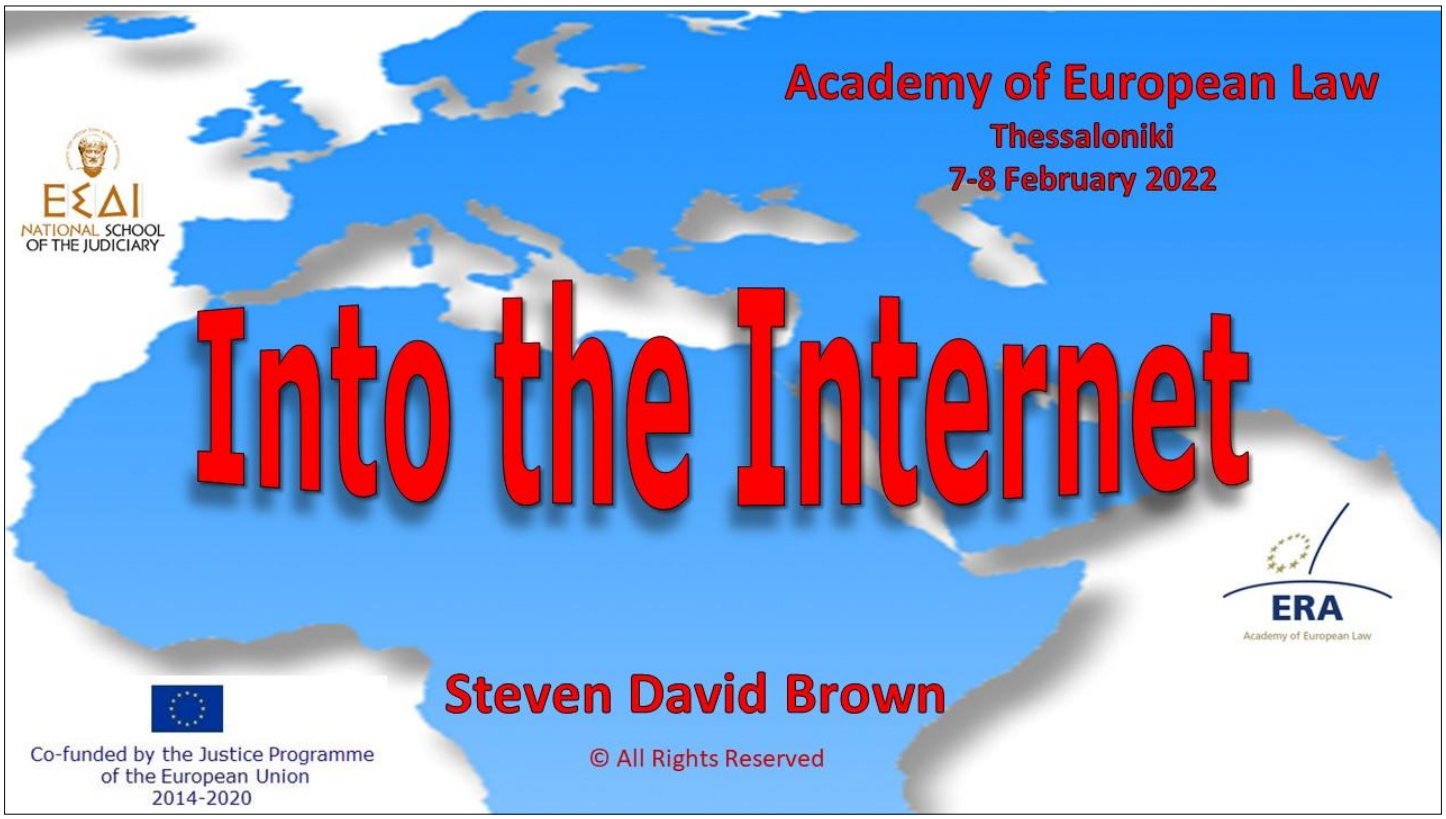
Language
English

Event number
322DT02f

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)



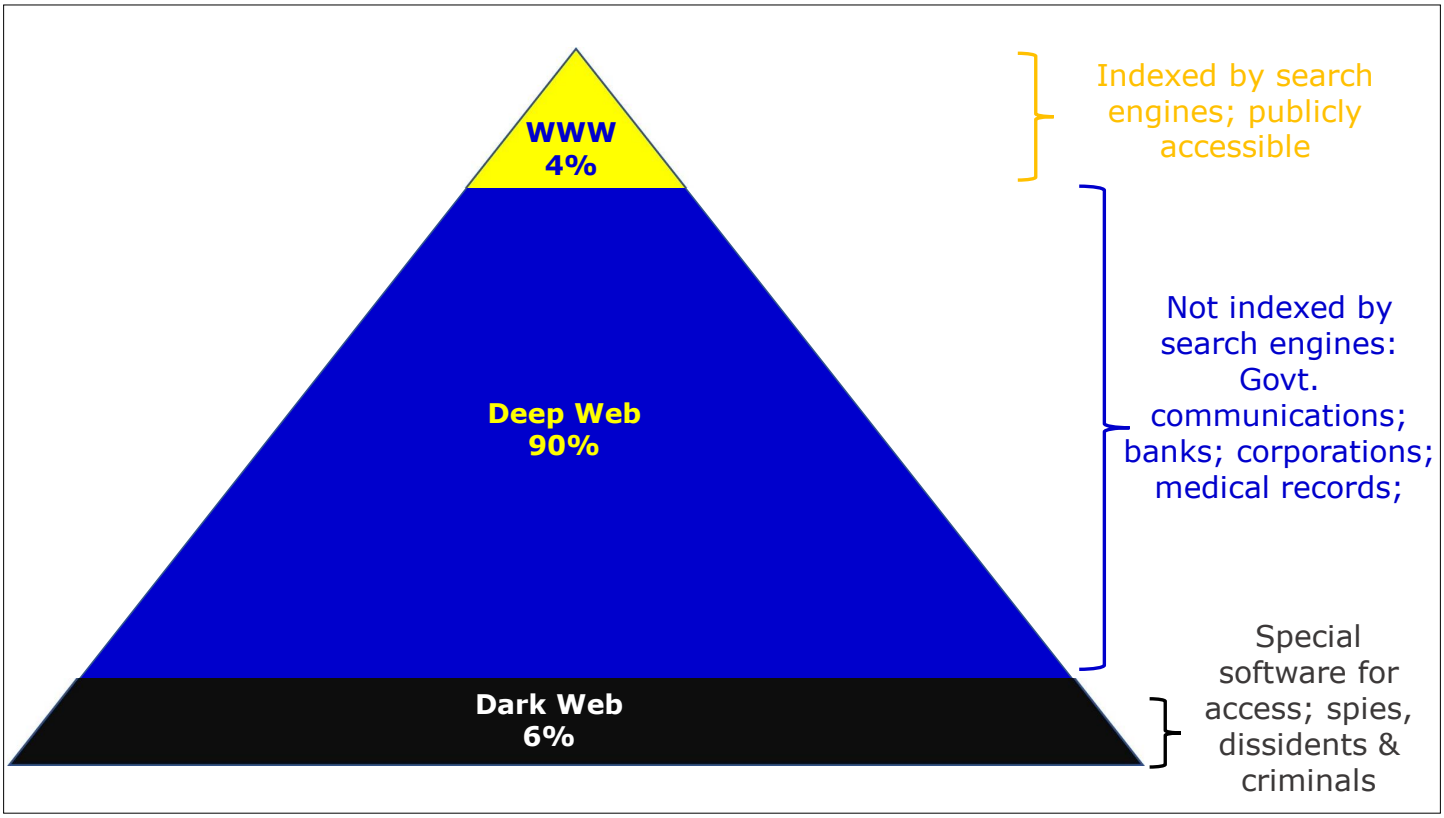

## What is the Internet ?

**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




## 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/

**WWW** contains **at least 4.13 billion pages**

( July 2021)

https://www.worldwidewebsize.com/

**2.5 quintillion bytes of data created daily**

(90% world's data created in the last two years)

https://www.the-next-tech.com/blockchain-technology/how-much-data-is-produced-every-day-2019/

A quintillion =1 followed by 18 zeros

**2,500,000,000,000,000,000 bytes per day**

**The Internet?**

**Insecure by design**

## 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**

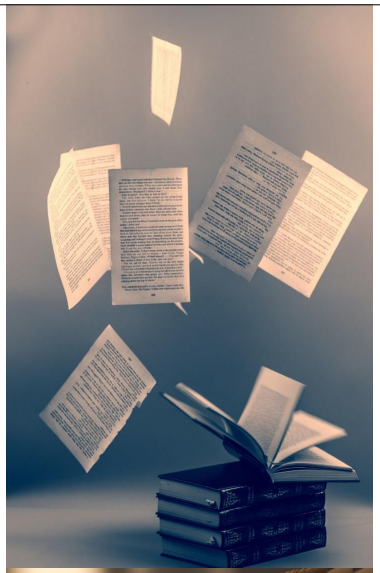
## HTTP & HTTPS (Hyper Text Transfer Protocol (Secure))

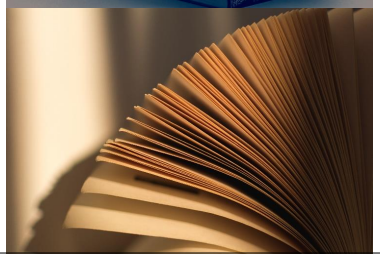
## Indexed 'pages'

## 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)



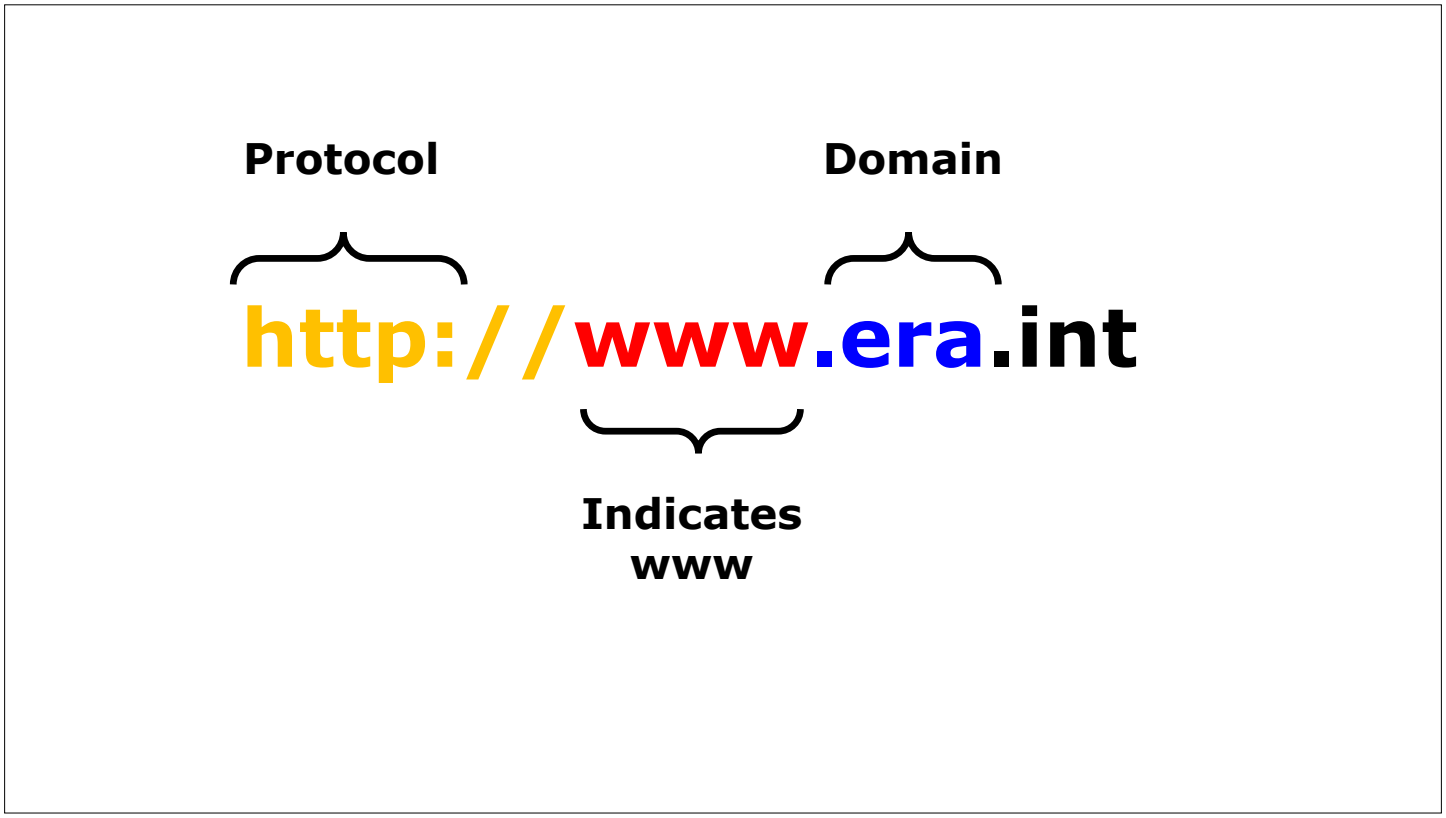


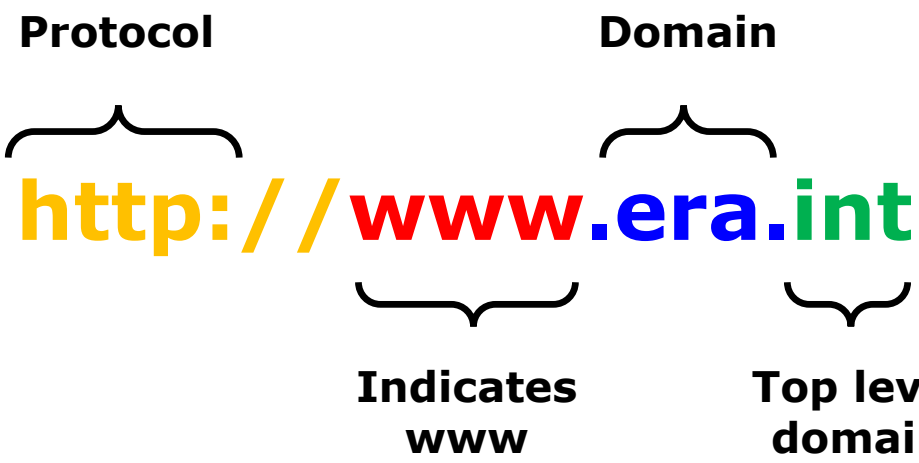
http://www.era.int

Protocol

http://www.era.int


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


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




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

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

# Whois

## Register of Internet domain name 'owners'

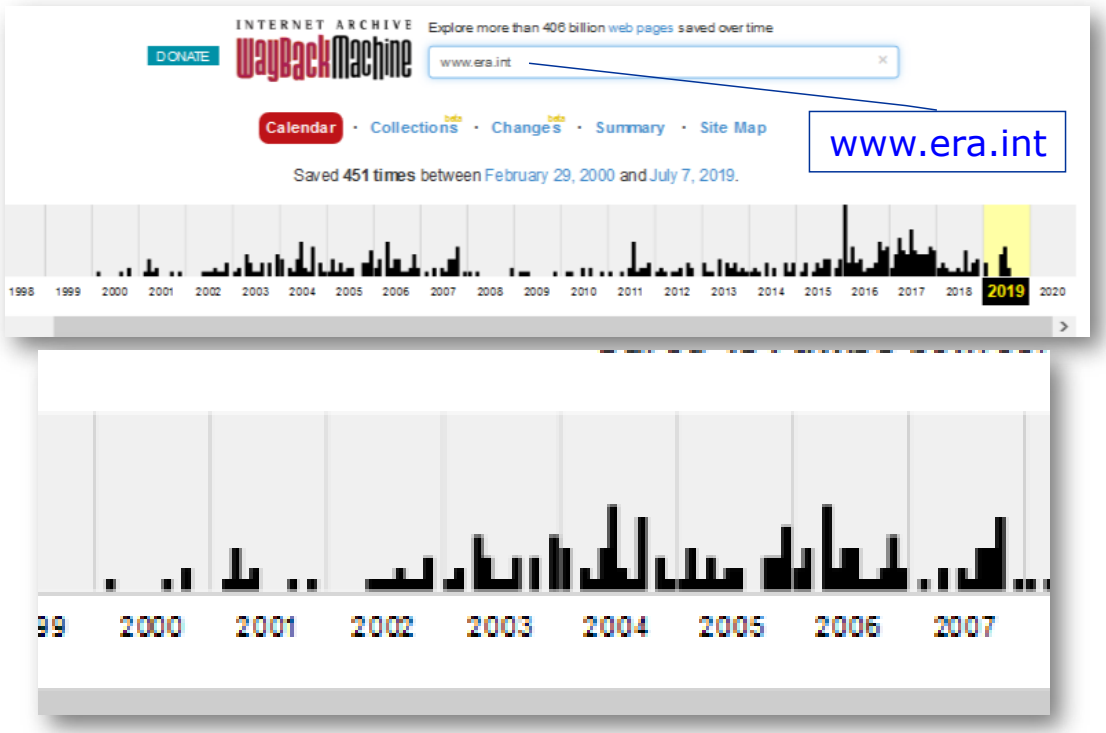
- Registrant data may be false
- Hidden behind a registration service
- Place to start search
- EU GDPR Rules – Whois blocked

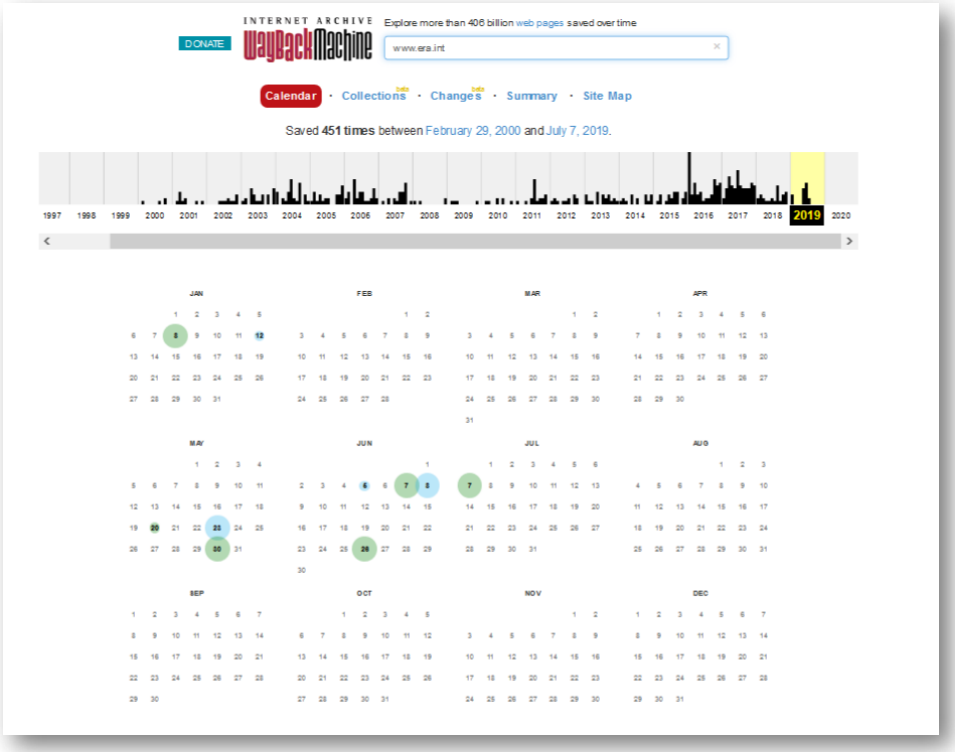
(Authorised groups still have access)

## When websites change:

INTERNET ARCHIVE
WayBackMachine

**(http://web.archive.org)**






# Website from 23 June 2000

## Normally:
## First step is to [illegible] the IP A[illegible]

*An Intern[illegible]dress is the uniq[illegible]ed by an Internet Se[illegible] and assigned to a co[illegible]vice to identify the source & dest[illegible]ion of messages sent across the Internet (like a postal address).*

**Can be faked, hidden or 'borrowed'**

# 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

**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**

**IP Address:**

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

**ISP holds records of usage**

## Be careful what you ask for …

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

## 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

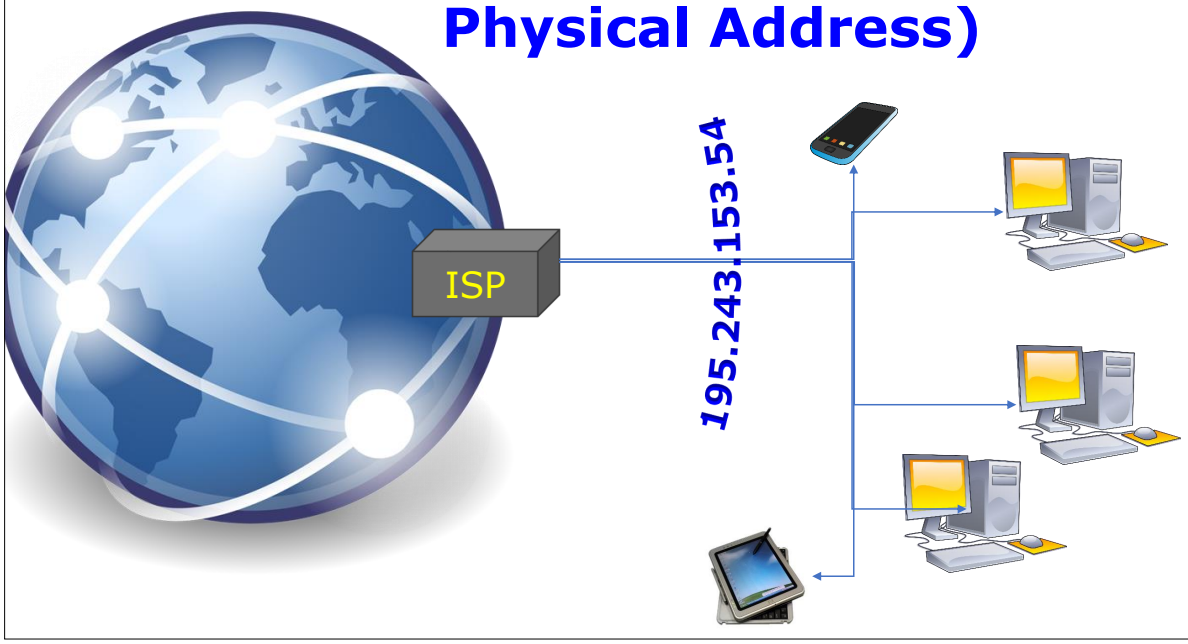
**"Blackmail to incite sexual acts by children over social media."**

**"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**

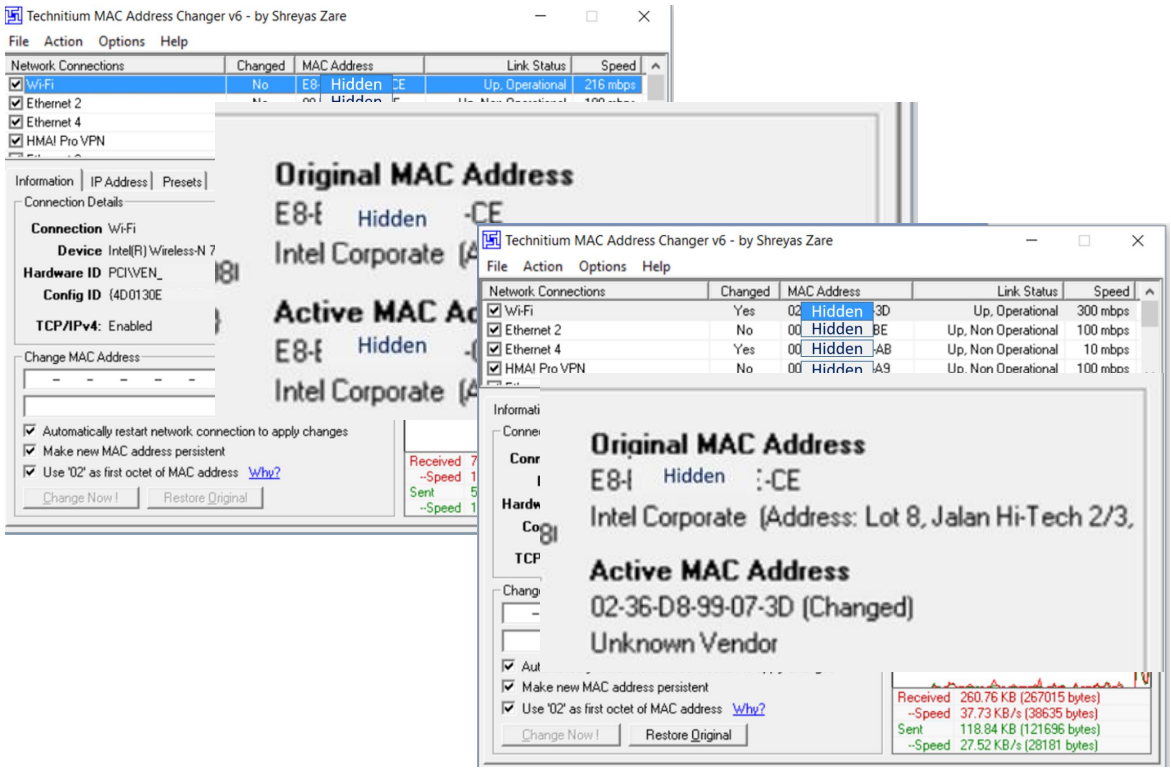
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/670219/IOCCO_annual_report_2016_2.PDF p74

# MAC Address: (Media Access Control or Physical Address)



# 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)



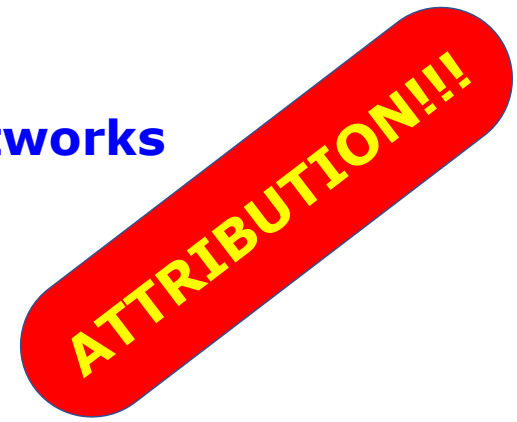
# Phones - IMEI

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#

# Hiding an IP

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

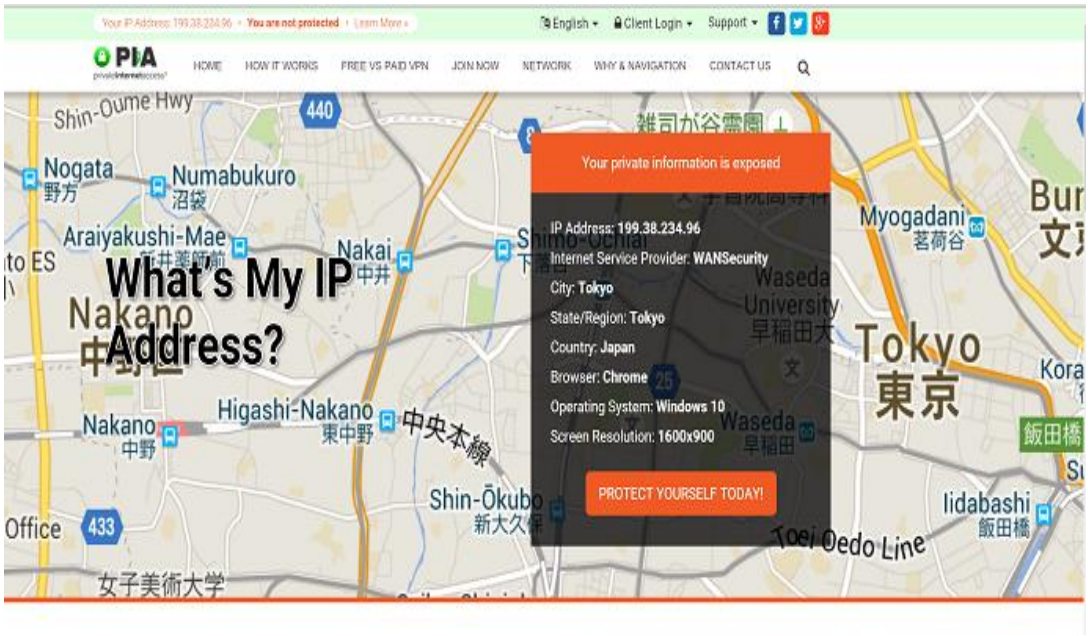


## 4 March 2015, California

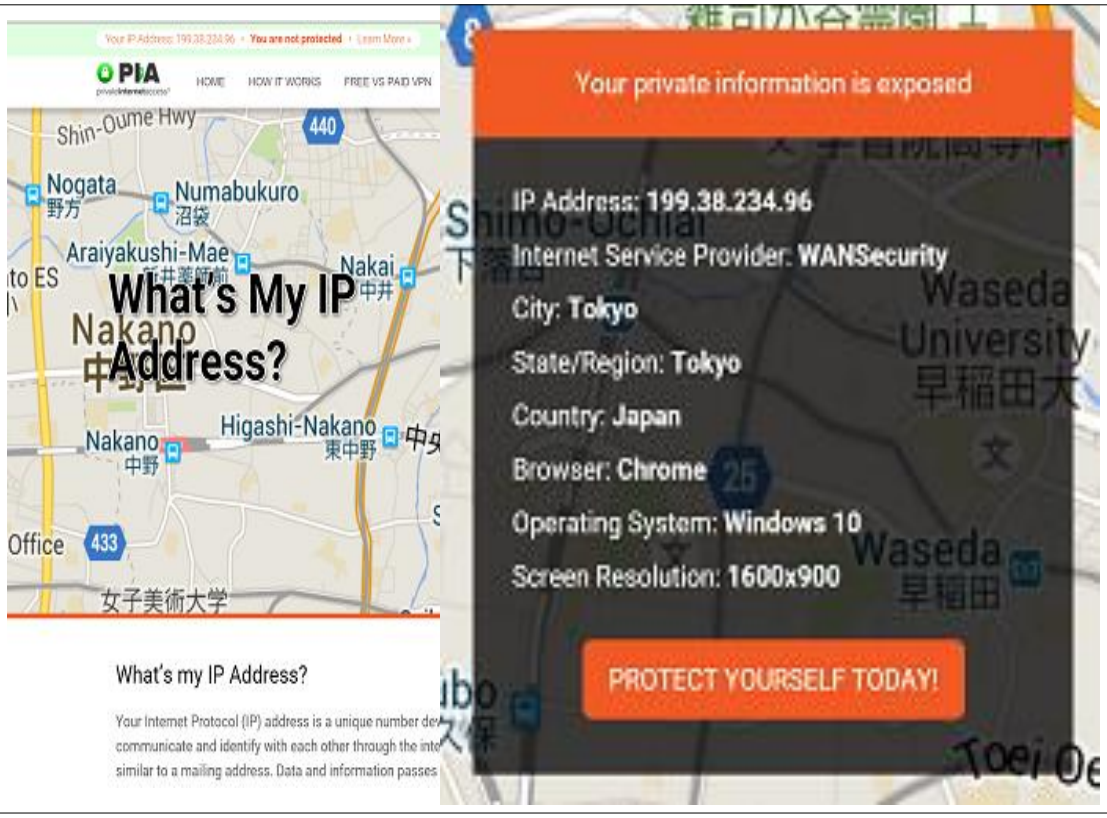
- Home burgled
- 65-inch Smart TV (with Netflix) stolen
- Victim realised someone using her Netflix account

**Bobby Alexander**

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




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



# 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!**

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

| | |
|---|---|
| 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 |

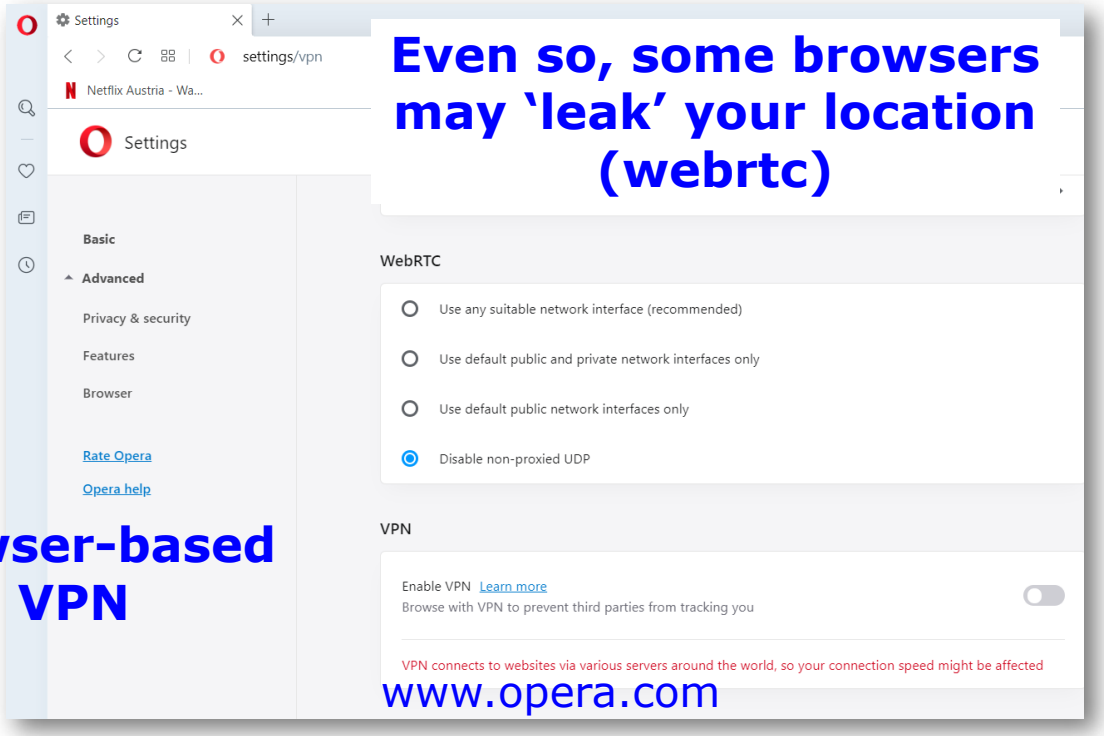
https://www.technadu.com/vpn-banned-countries-list/7432/

## Well known VPN providers:

**ExpressVPN**
**NordVPN**
**Hidemyass**
**CyberGhost VPN**
**Proton VPN**

**Included in some anti-virus/internet security packages**

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




**Browser-based VPN**

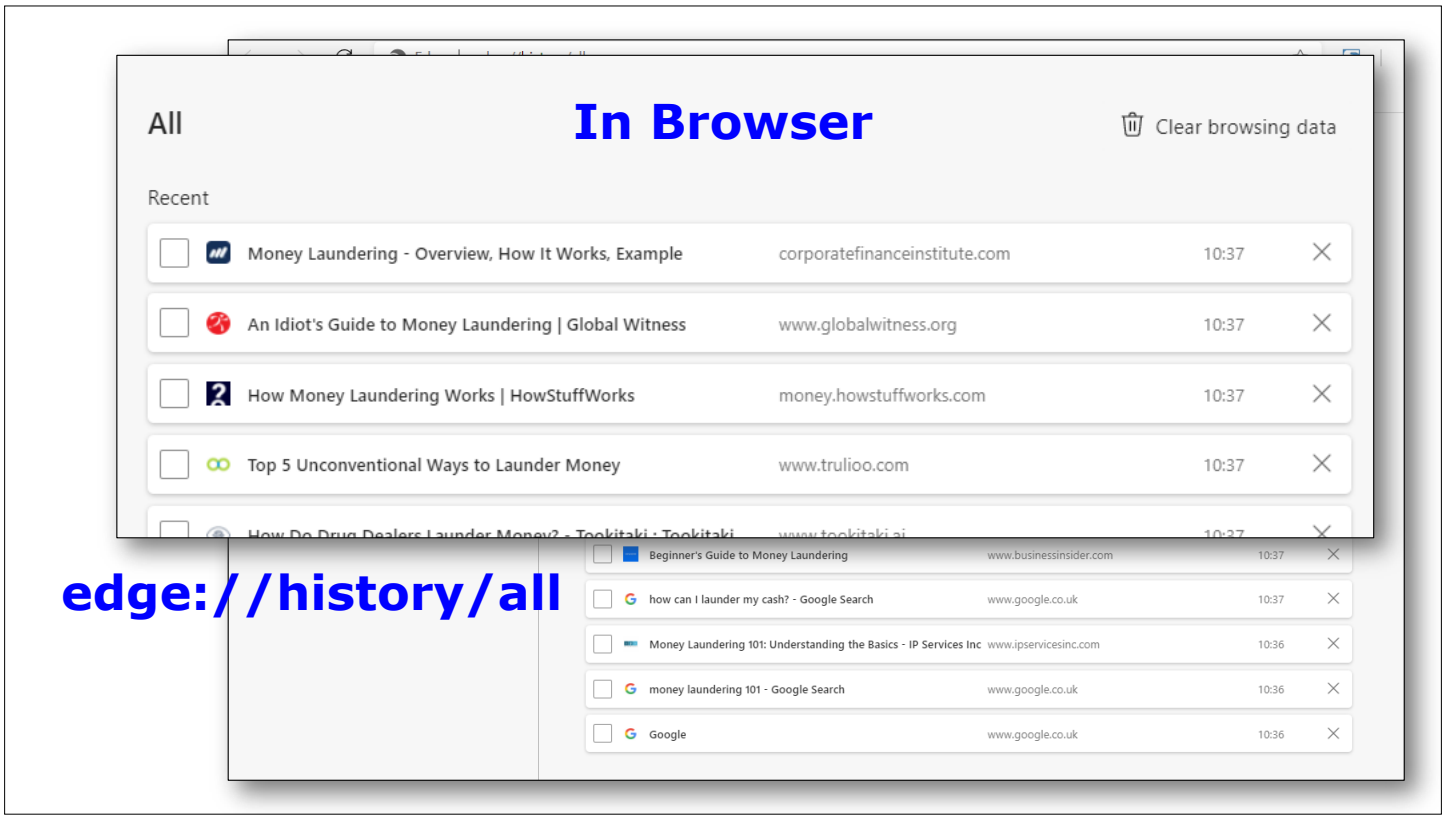
www.opera.com

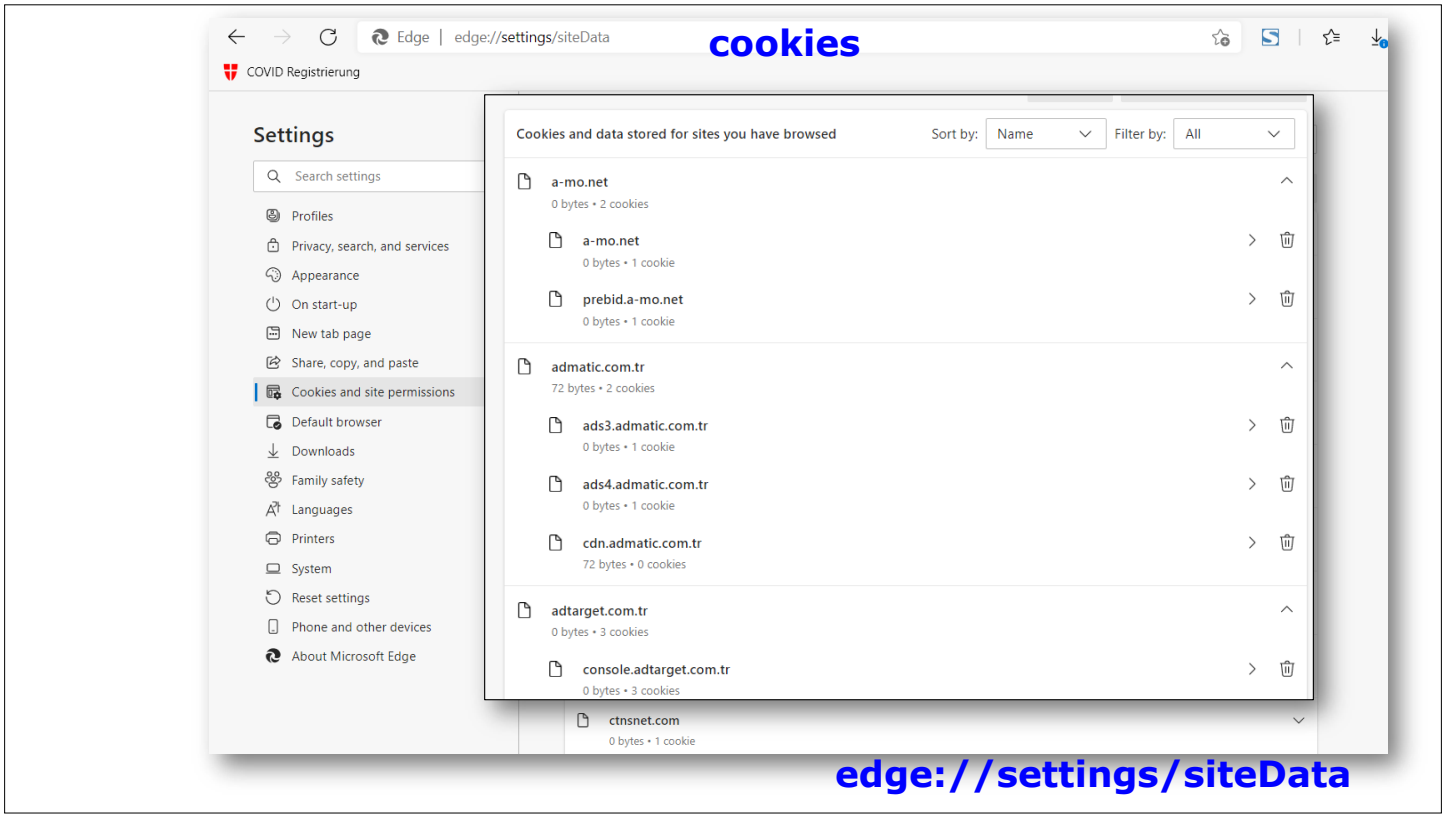
Settings/Advanced/Privacy & security/

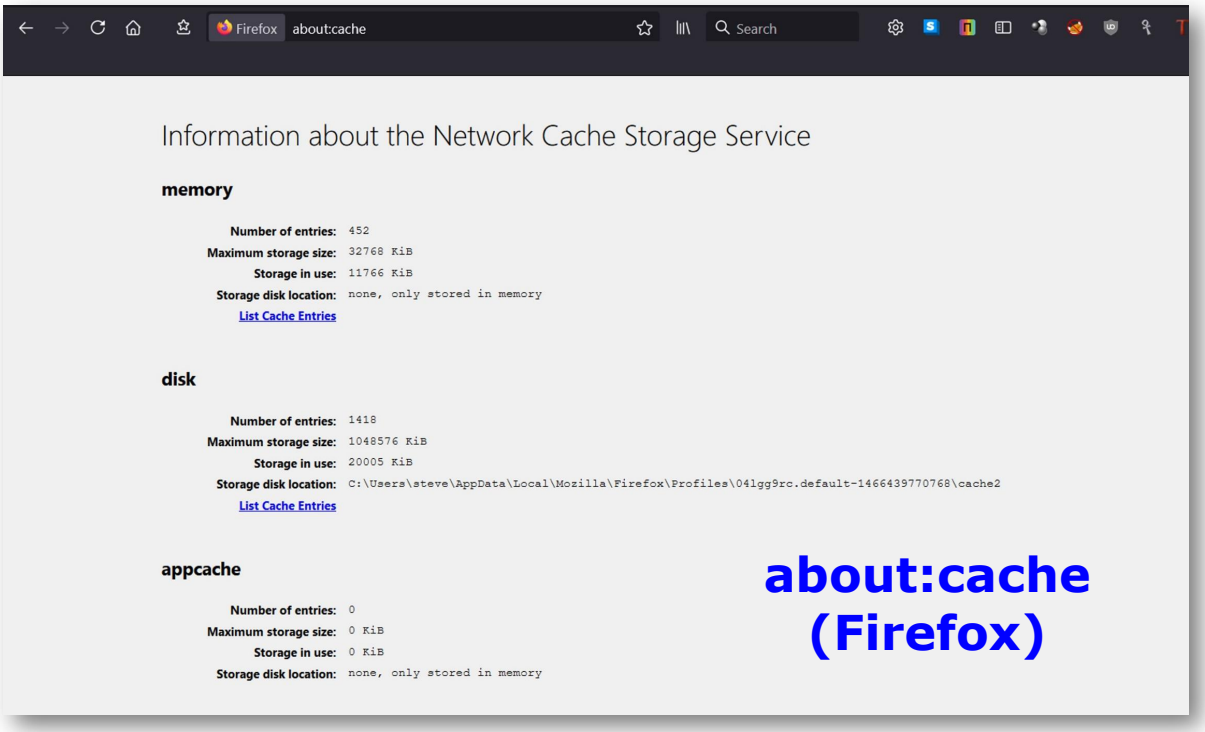
# All you need is logs

## LOGS

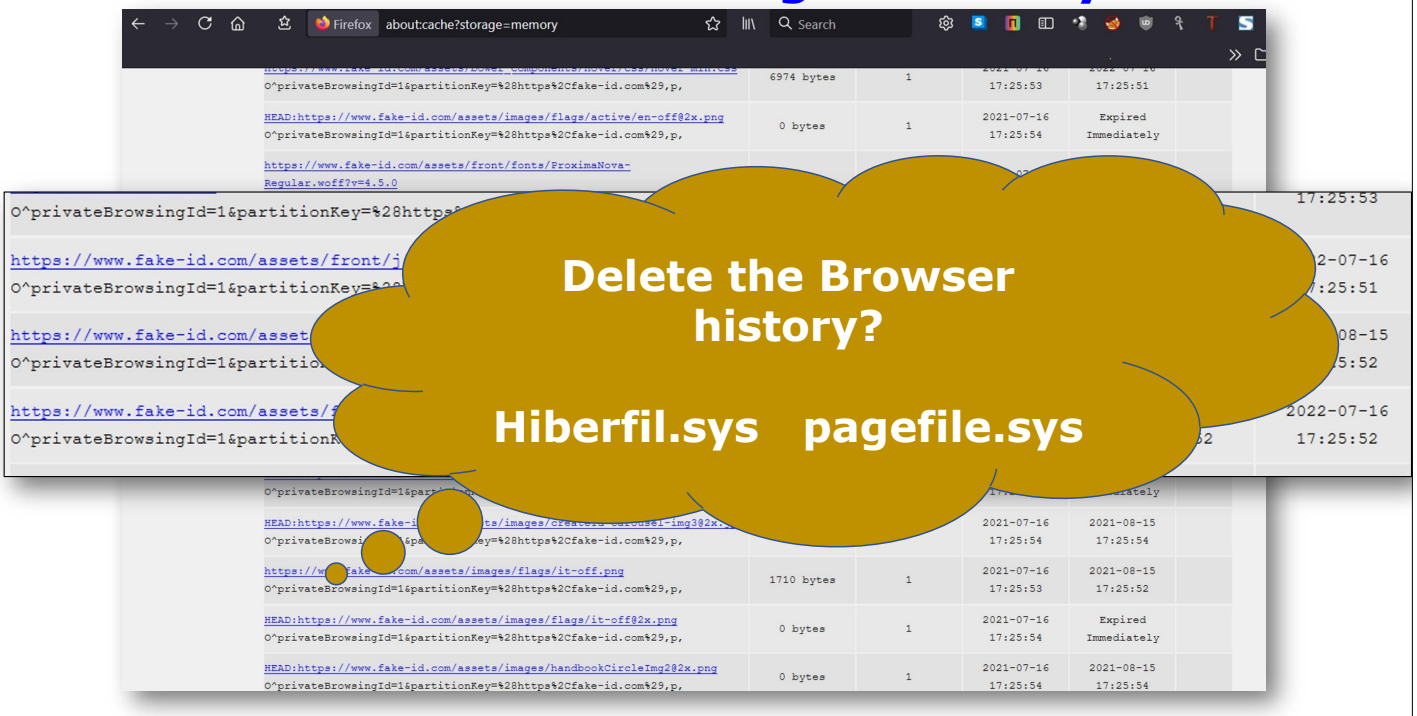
- Originally created for tracing bugs & improving performance
- Billing/maintenance records
- Generated automatically
- On the device
- On servers in the network
- Service providers
- Record meta-, traffic-data


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


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




# about:cache?storage=memory



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

**Username weirdo0000**

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

**Encrypted chats discussed with seller:**

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

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

**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

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

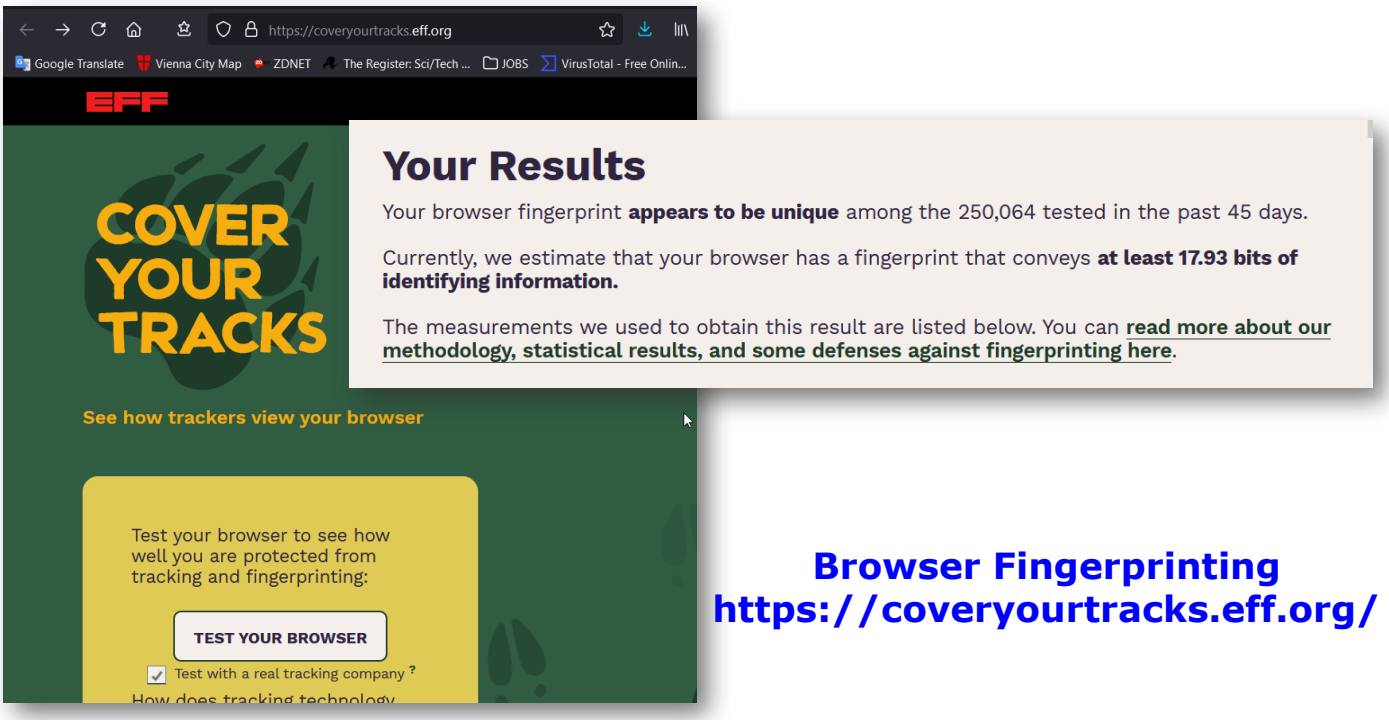
## Try this out:

## https://webkay.robinlinus.com/

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

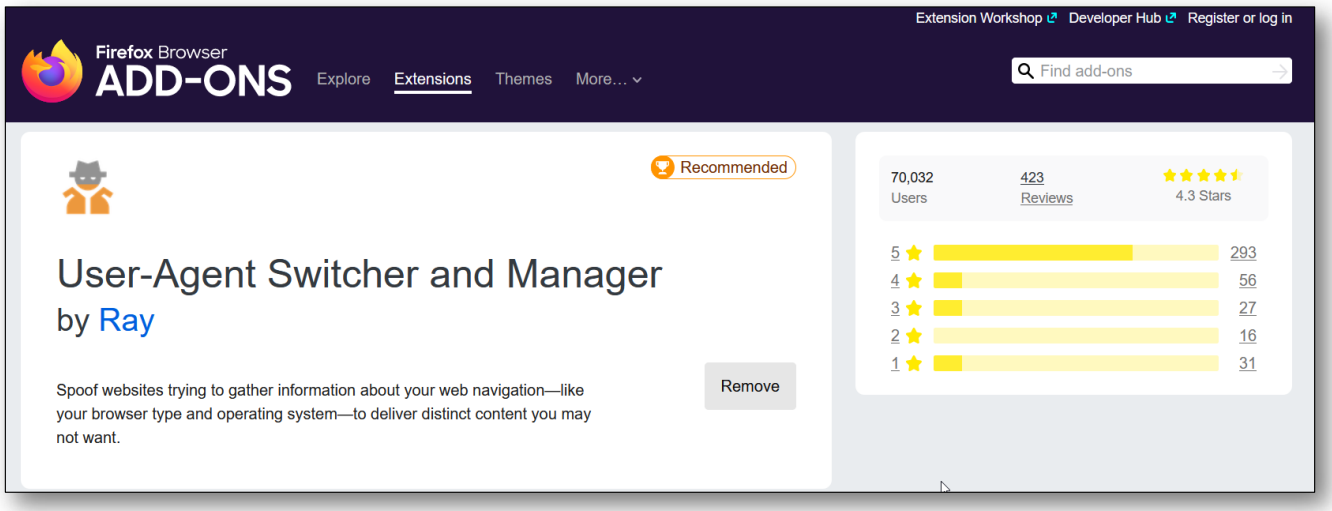

**'In 2017, both Alphabet (Google's parent company) and Facebook made an overwhelming majority of their total profits through digital advertising—88% and 97%, respectively.'**

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

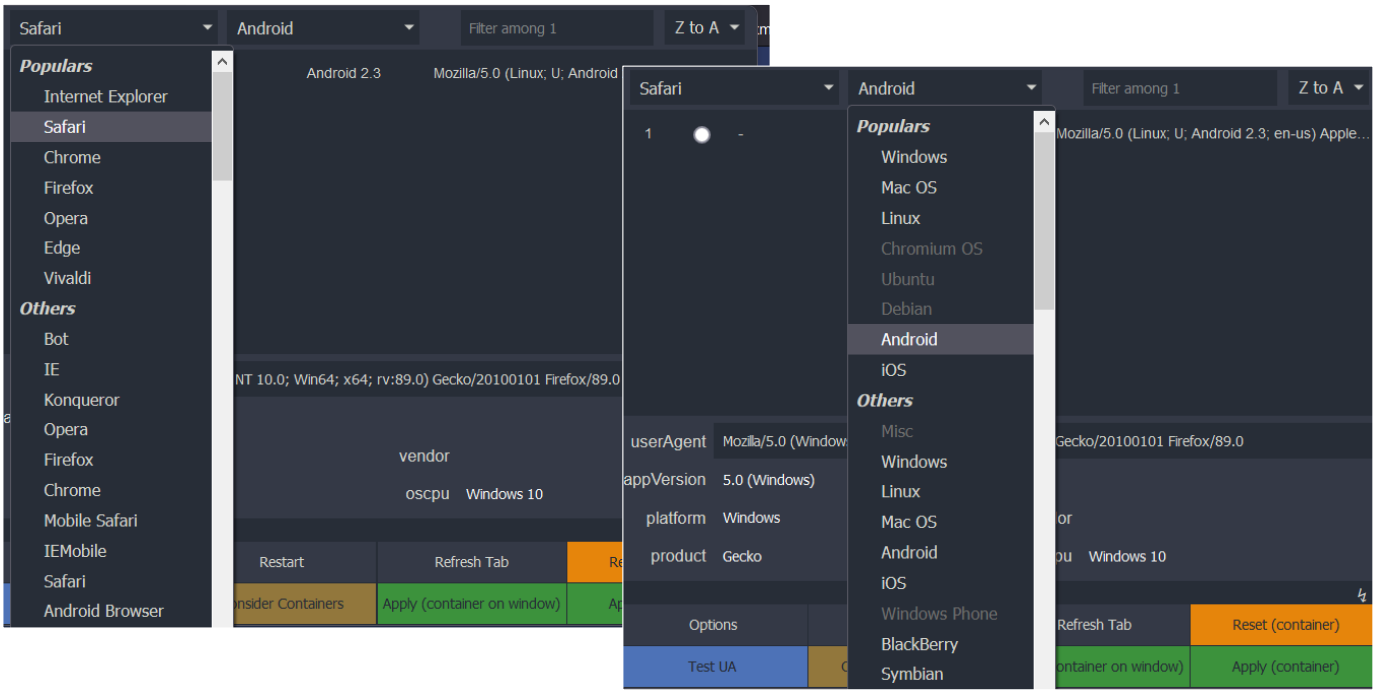



**Browser Fingerprinting**
**https://coveryourtracks.eff.org/**

## Browser fingerprint can also be faked:



## Browser fingerprint can also be faked:




**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**

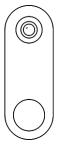
**Relocated for business reasons (like load or electricity prices)**

**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**





# IOT

## Estimated 22 billion -50 billion devices

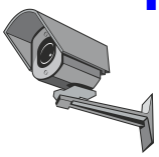
## All connected


## All generating & logging data



# 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/


No central control

All websites end with .onion

Can be used to access DarkNet

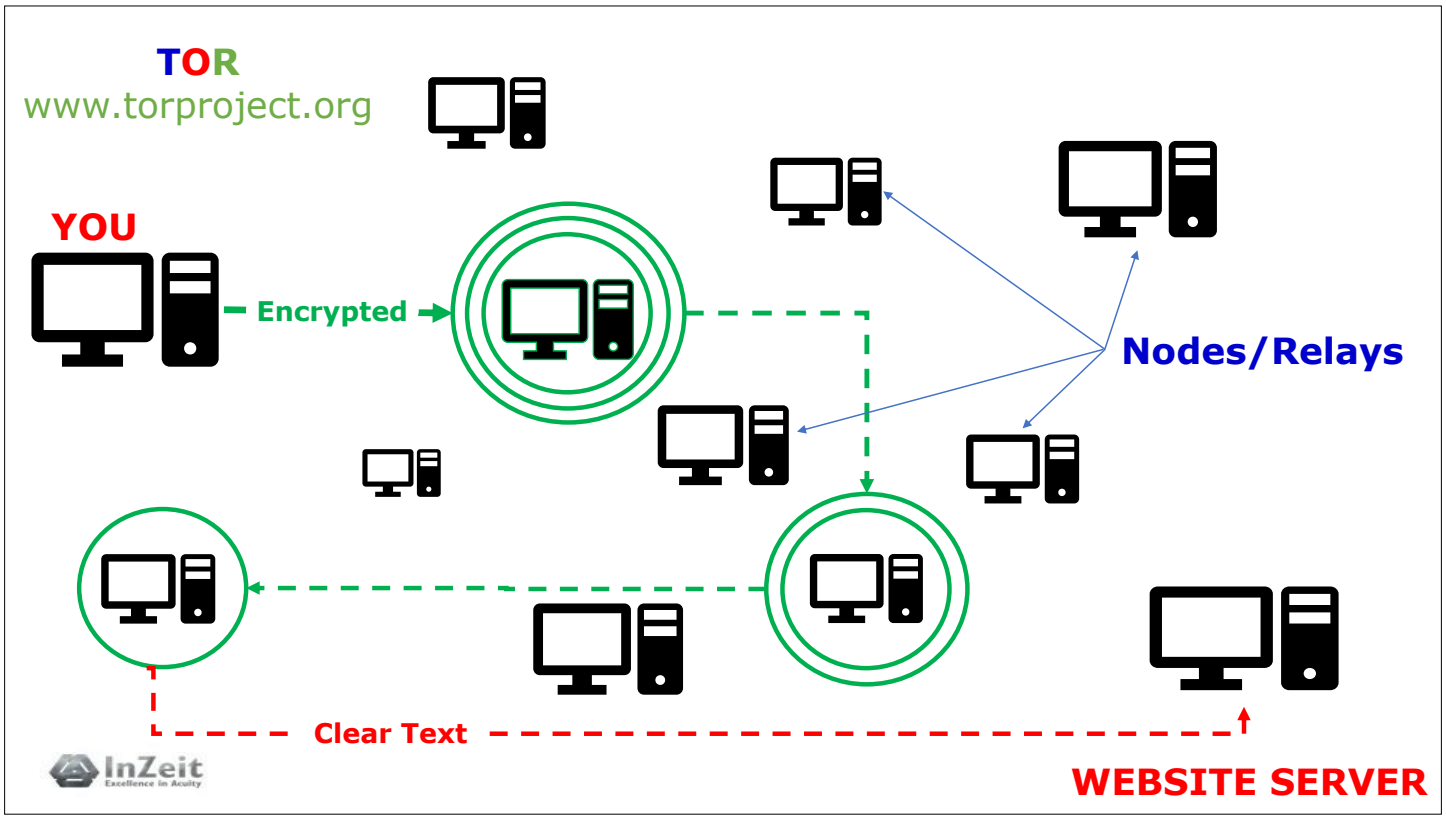
# TOR

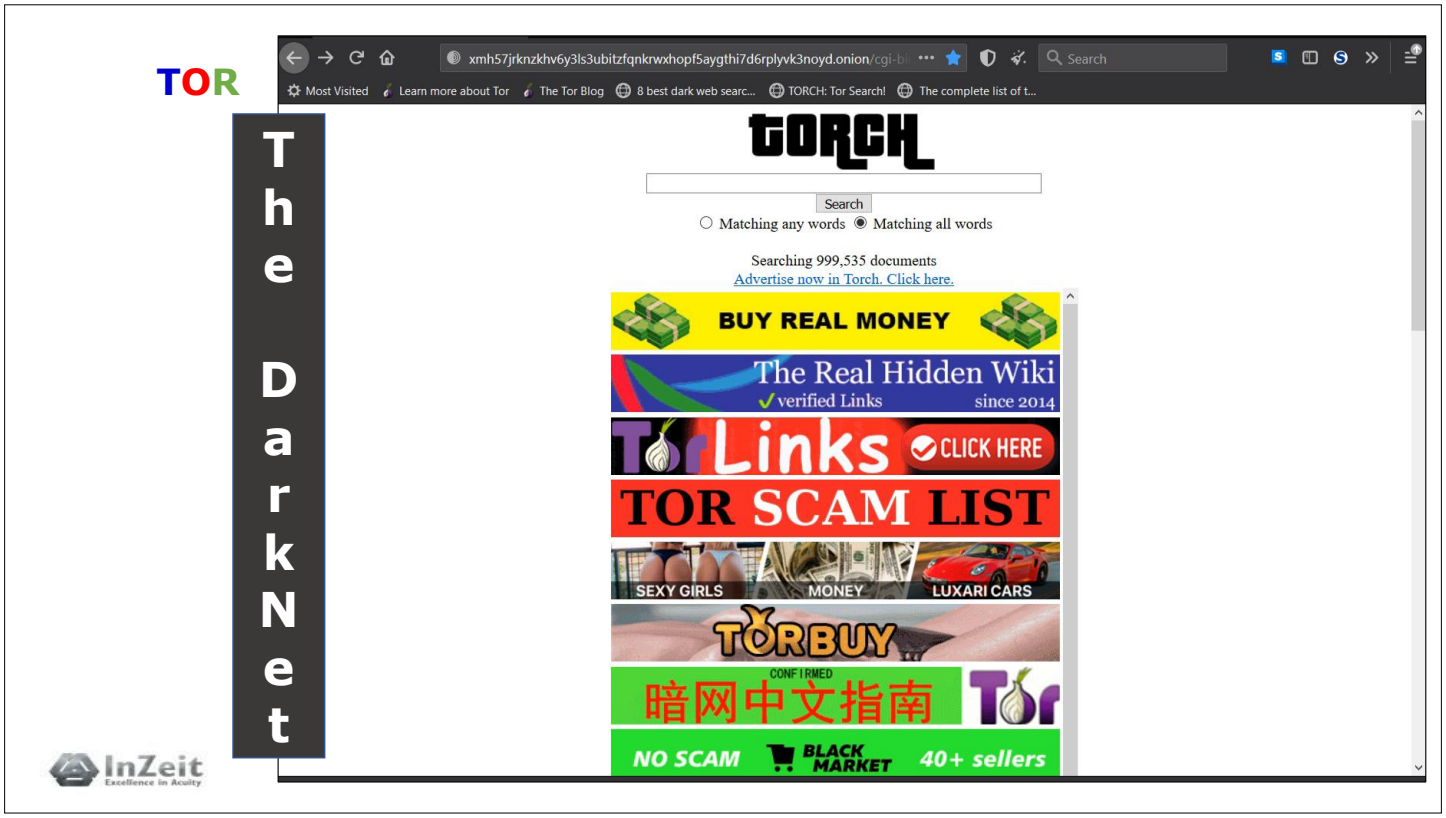
## The Onion Router

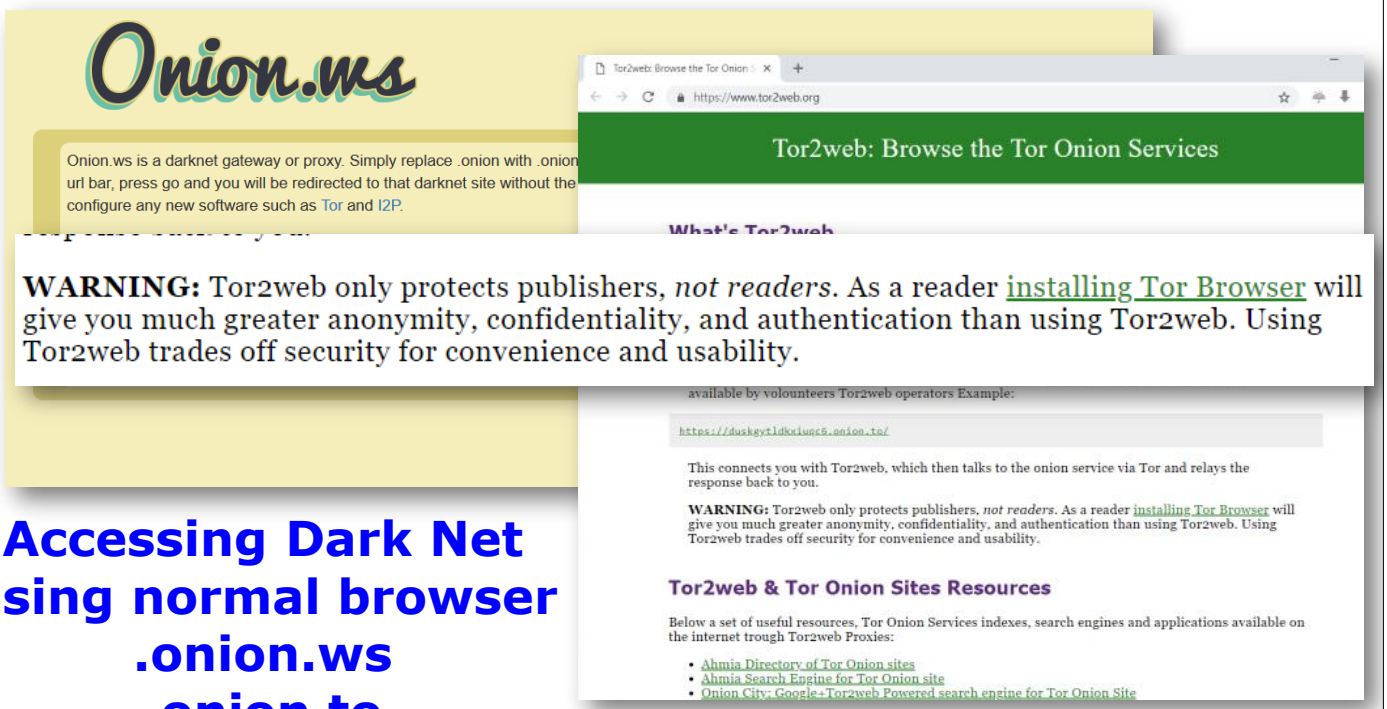
Peer to Peer Network (people volunteer part of their hard drive)

'Anonymising technology' (there are others)

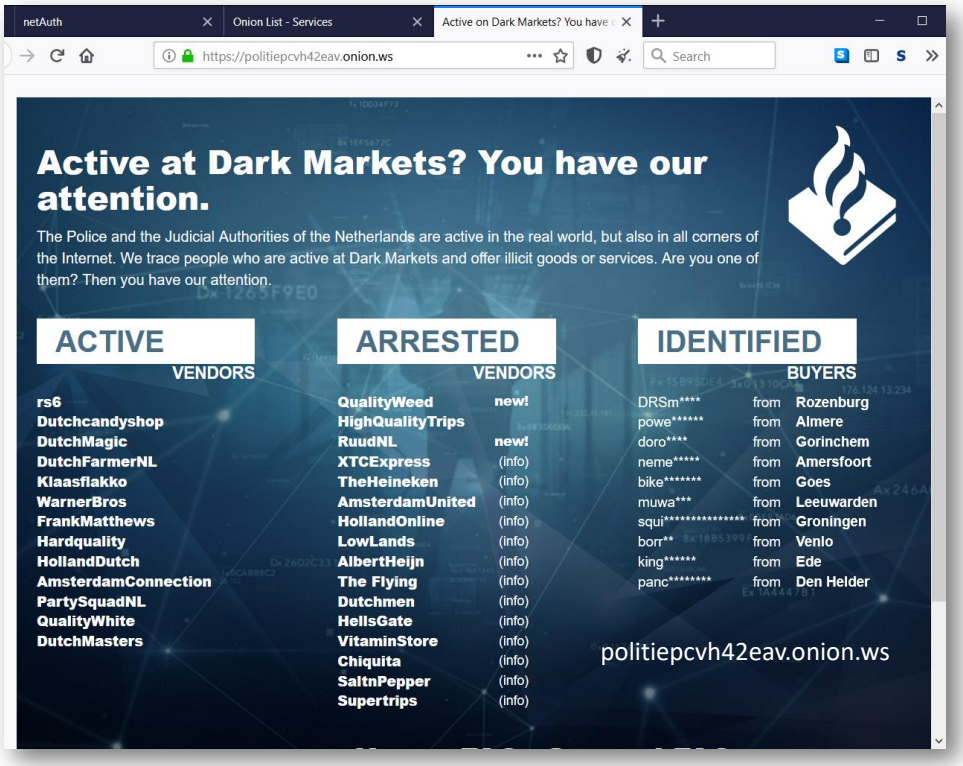
InZeit
Excellence in Acuity

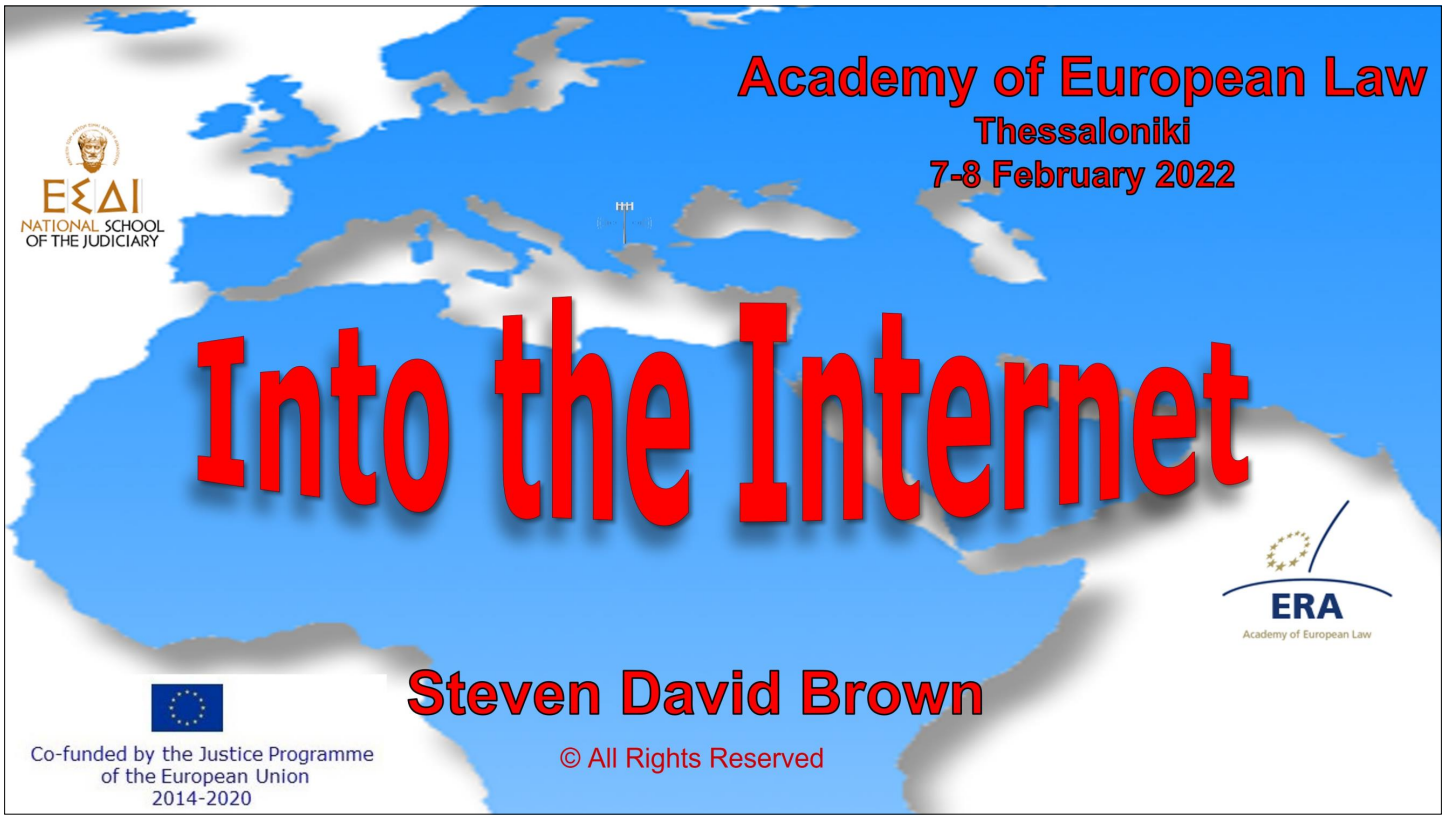

TOR
www.torproject.org
YOU
Encrypted
Nodes/Relays
Clear Text
WEBSITE SERVER
InZeit


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




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




Academy of European Law
Thessaloniki
7-8 February 2022
ΕΣΔΙ
NATIONAL SCHOOL
OF THE JUDICIARY
Into the Internet
ERA
Academy of European Law
Steven David Brown
Co-funded by the Justice Programme
of the European Union
2014-2020
© All Rights Reserved

energie, technologie en optimisme

# Open-source tools, computer forensics on mobile devices and in the "Cloud"

07/02/2022

Co-funded by the Justice Programme of the European Union 2014-2022

1

## Introduction

- Remco Sprooten
- Team leader for the ENGIE SDO Security operations center
- Team leader for the SDO Red Team
- Former digital forensic investigator for the Dutch Police
- Activities include:
  - Ethical hacking (penetration testing)
  - Freelance malware research
  - Incident responder

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

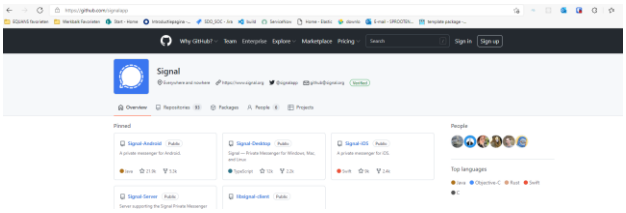
Co-funded by the Justice Programme of the European Union 2014-2022



2

# Open Source

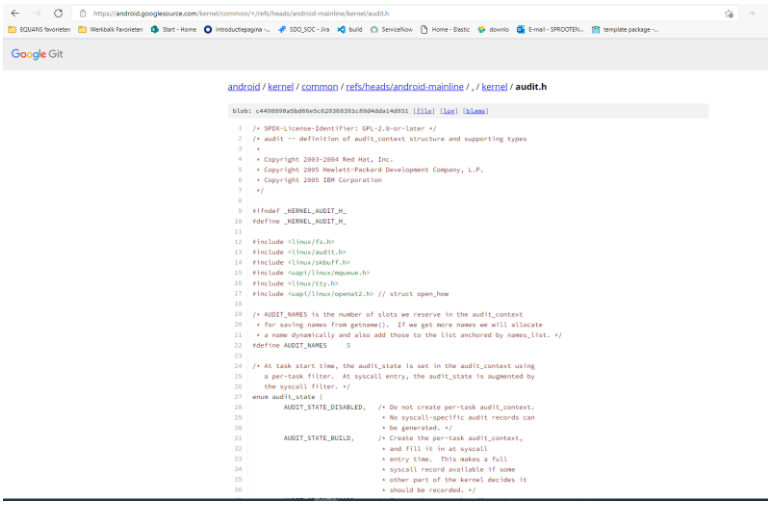
- What is open source?
  - Open source is source code that is made freely available for possible modification and redistribution. Products include permission to use the source code, design documents, or content of the product.
- Well known examples
  - Android
  - Linux
  - Signal
  - BSD






3

# Open Source - Android






4

# GPL License

…
In purely private (or internal) use—with no sales and no distribution—the software code may be modified and parts reused without requiring the source code to be released. For sales or distribution, the entire source code needs to be made available to end users, including any code changes and additions
…



5

# Encryption and privacy (basics)

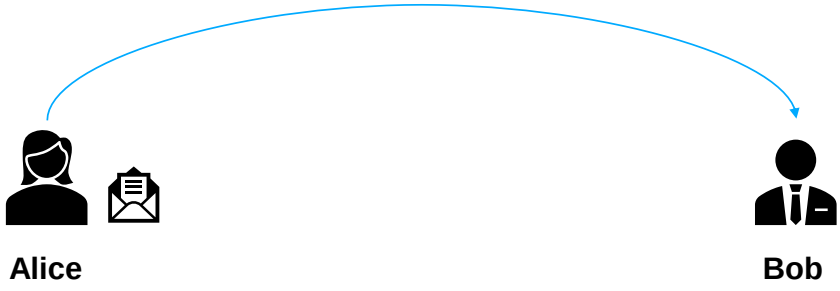
**Alice**

**Bob**



6

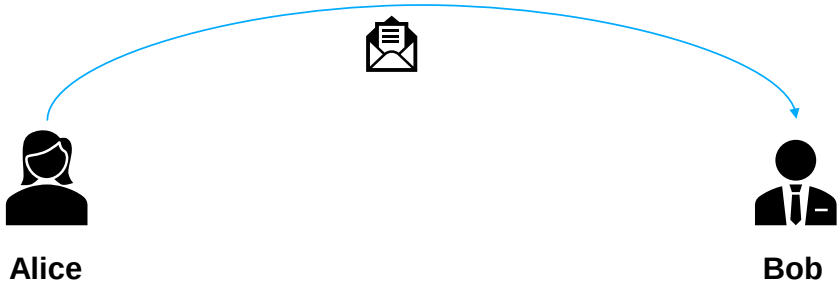
# Encryption and privacy (basics)






7

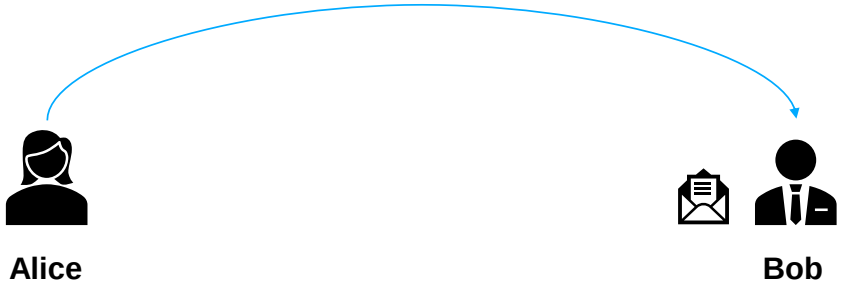
# Encryption and privacy (basics)






8

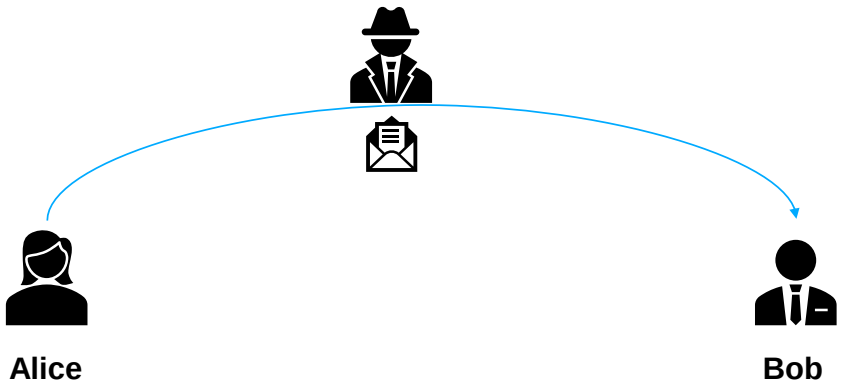
# Encryption and privacy (basics)






9

# Encryption and privacy (basics)





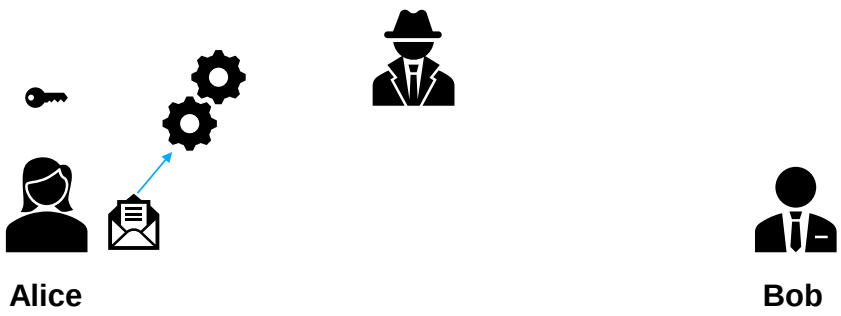

10

# Encryption and privacy (basics)




11

# Encryption and privacy (basics)






12

# Encryption and privacy (basics)




13

# Encryption and privacy (basics)



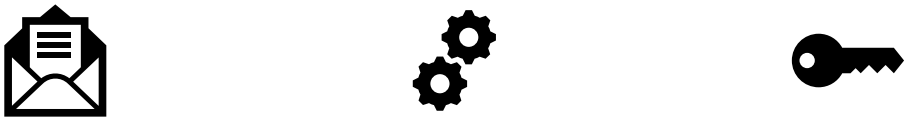

14

# Encryption and privacy (basics)




15

# Encryption and privacy (basics)



Message | Encryption algorithm | Key



16

# Encryption and privacy (basics)


Ciphertext | Encryption algorithm | Key



17

# Encryption and privacy (basics)

**Ciphertext: The encrypted message**

- Is assumed to be known

**Encryption algorithm**

- Is assumed to be known

**The key**

- Should be kept private



18

# Encryption and privacy (basics)

11101
01010
11101
01010
10101
01110
10101
01010
10

Ciphertext

Encryption algorithm

Key



19

# Encryption and privacy (basics)

## Symmetric encryption

- A key for encrypting and decrypting is the same.
- Ex. AES, 3DES

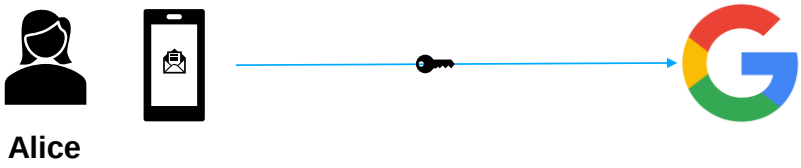
## Asymmetric encryption

- A key for encrypting and a key for decrypting
- Ex. RSA, DSA, EC



20

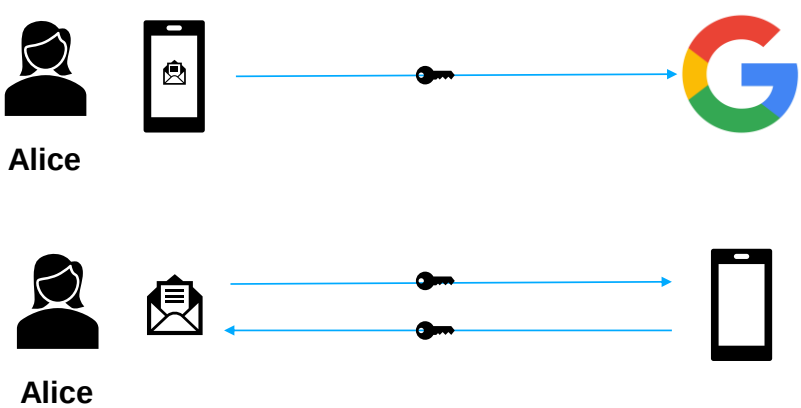
# Encryption on smartphones






21

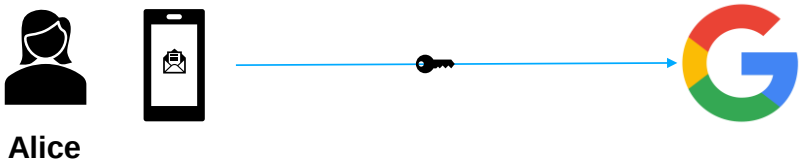
# Encryption on smartphones



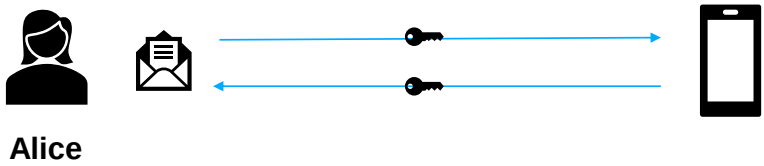



22

# Encryption on smartphones




Key is agreed upon during the connection




Key is based on the PIN/Password cobined with the device



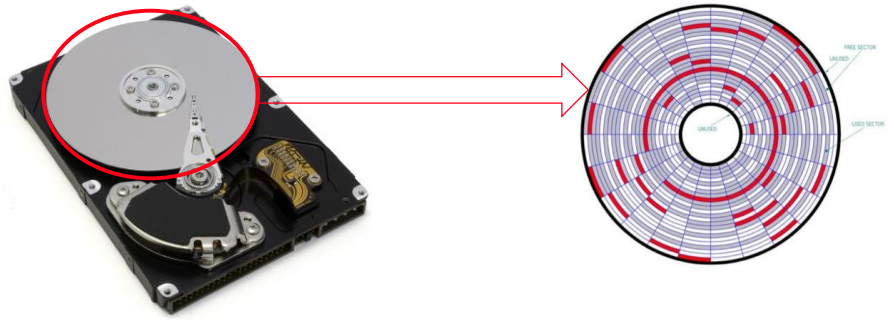
23

# Physical Extraction



24

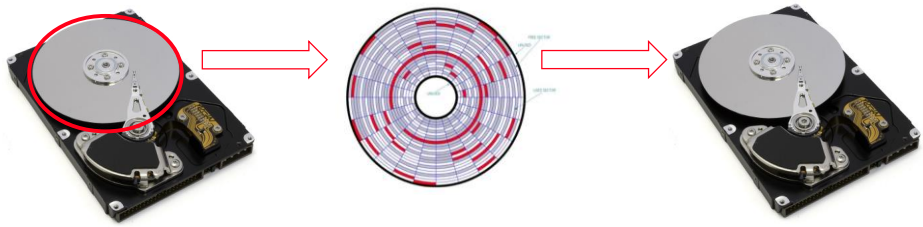
# Physical Extraction





25

# Physical Extraction





26

# Physical to Logical

- New storage technology
  - Solid stade drives (SSD)
  - Flash memory
- Data is no longer stored in predictical locations
- Computers / devices still rely on these locations



27

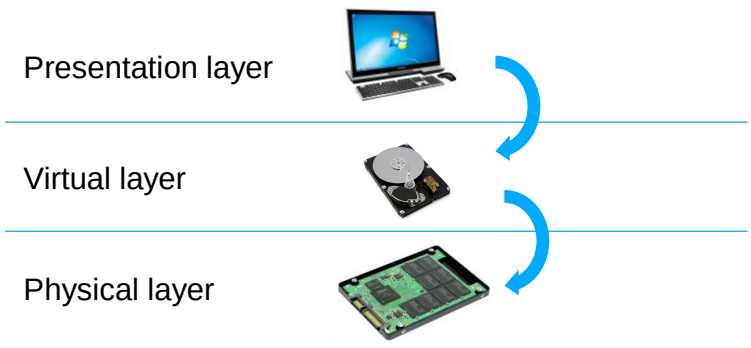
# Physical to Logical

- New storage technology
  - Solid stade drives (SSD)
  - Flash memory
- Data is no longer stored in predictical locations
- Computers / devices still rely on these locations
- Physical is less physical



28

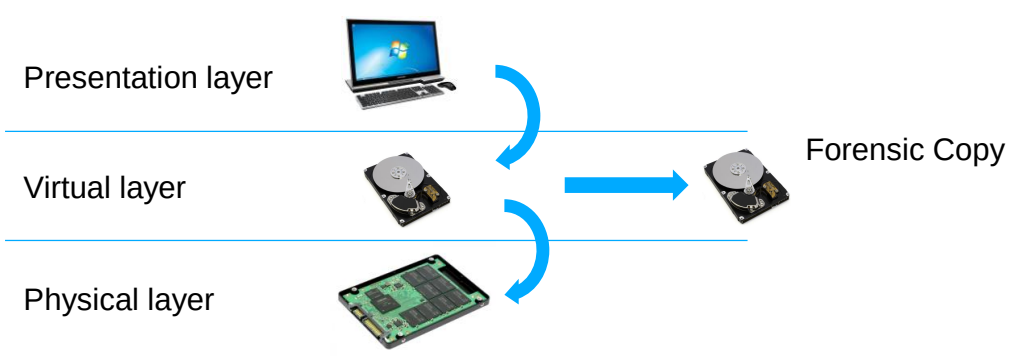
# Physical to Logical






29

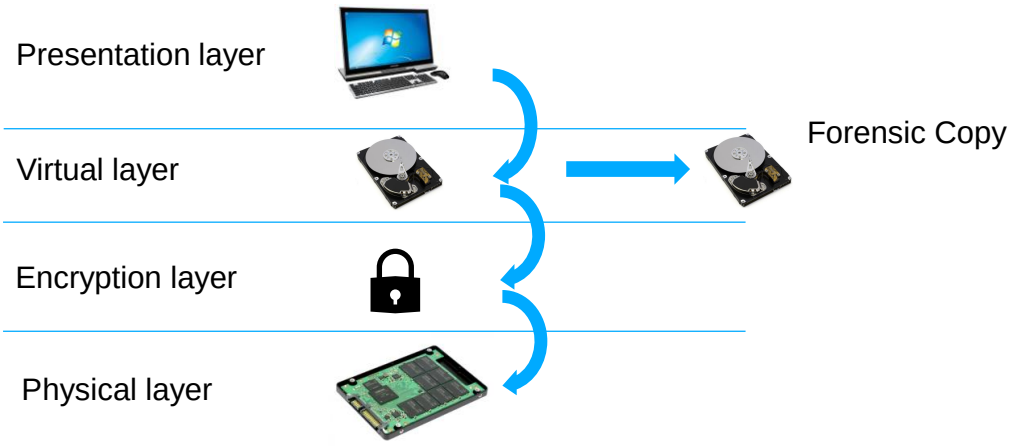
# Physical to Logical






30

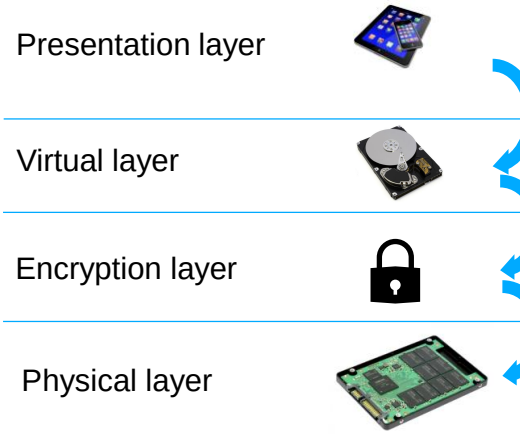
# Physical to Logical






31

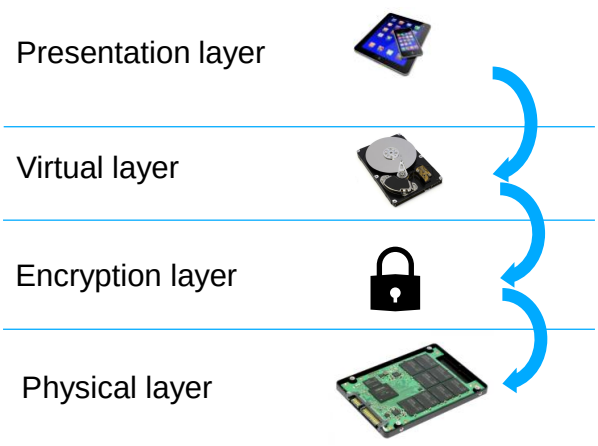
# Physical to Logical






32

# Physical to Logical

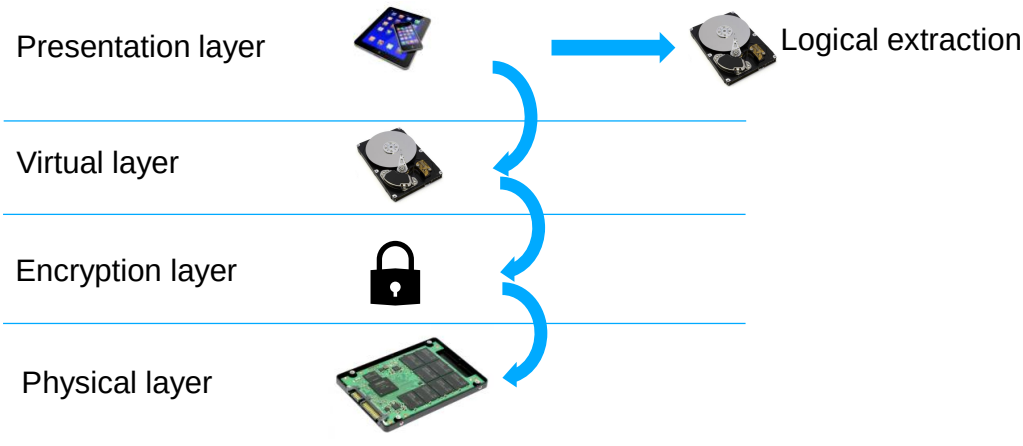



Mobile devices add extra (security) layers



33

# Physical to Logical






34

# Logical Extractions

Presentation layer 

Virtual layer 

Encryption layer 

Physical layer 

Lost information:
- Physical data location



35

# Physical to Logical

Presentation layer 

Virtual layer 

Encryption layer 

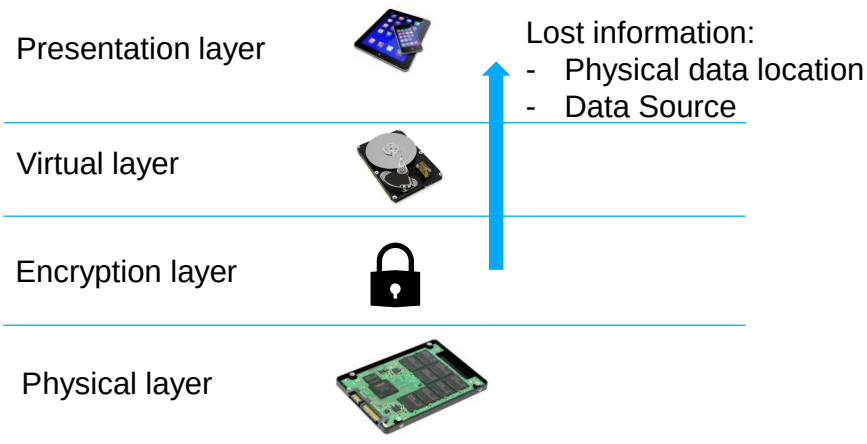
Physical layer 

Lost information:
- Physical data location



36

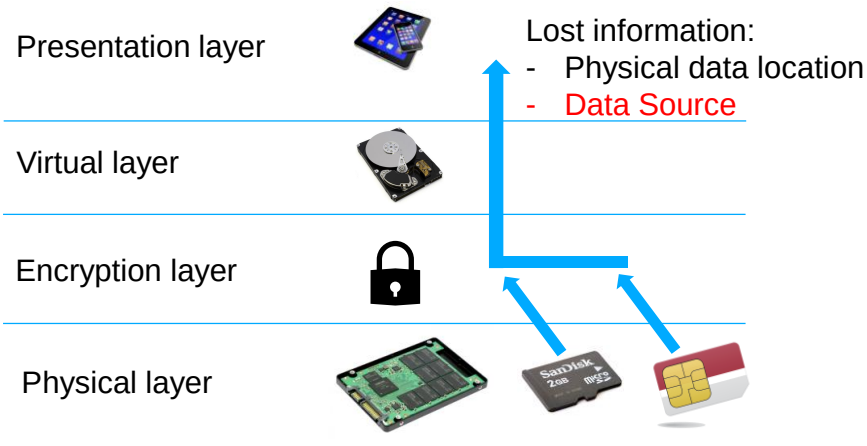
# Physical to Logical






37

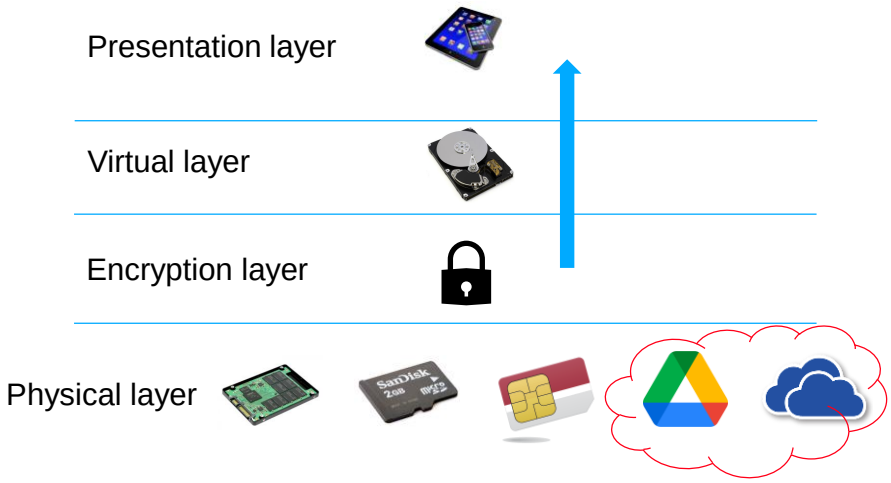
# Physical to Logical






38

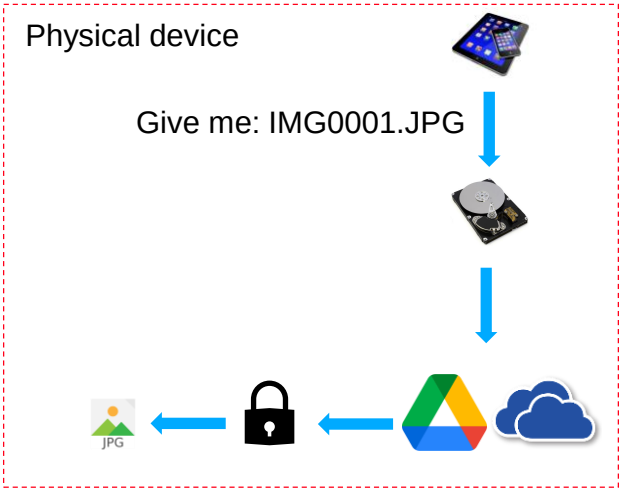
# Physical to Logical






39

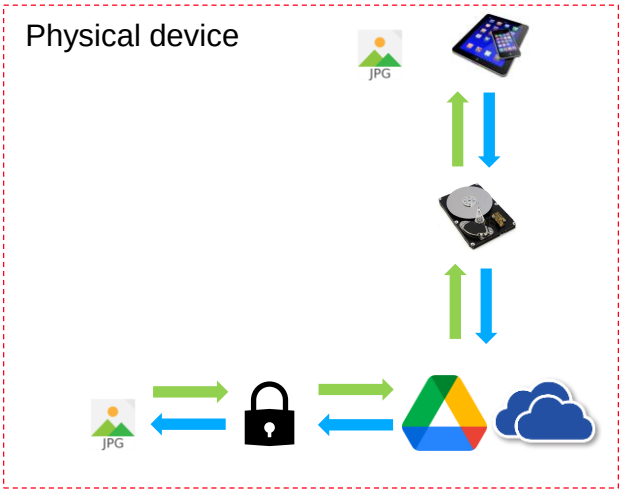
# Physical to Logical






40

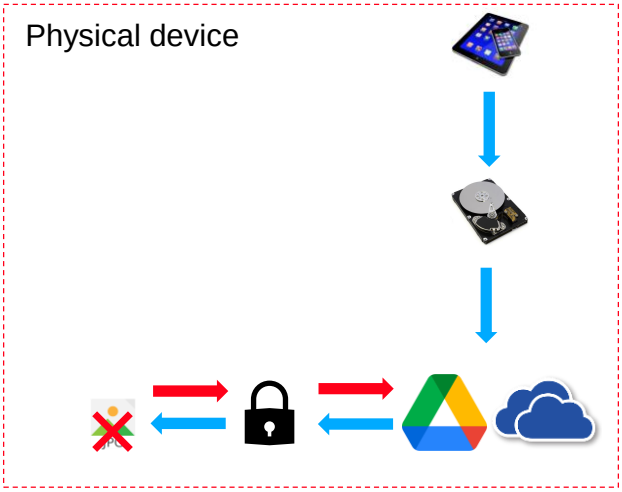
# Physical to Logical






41

# Physical to Logical

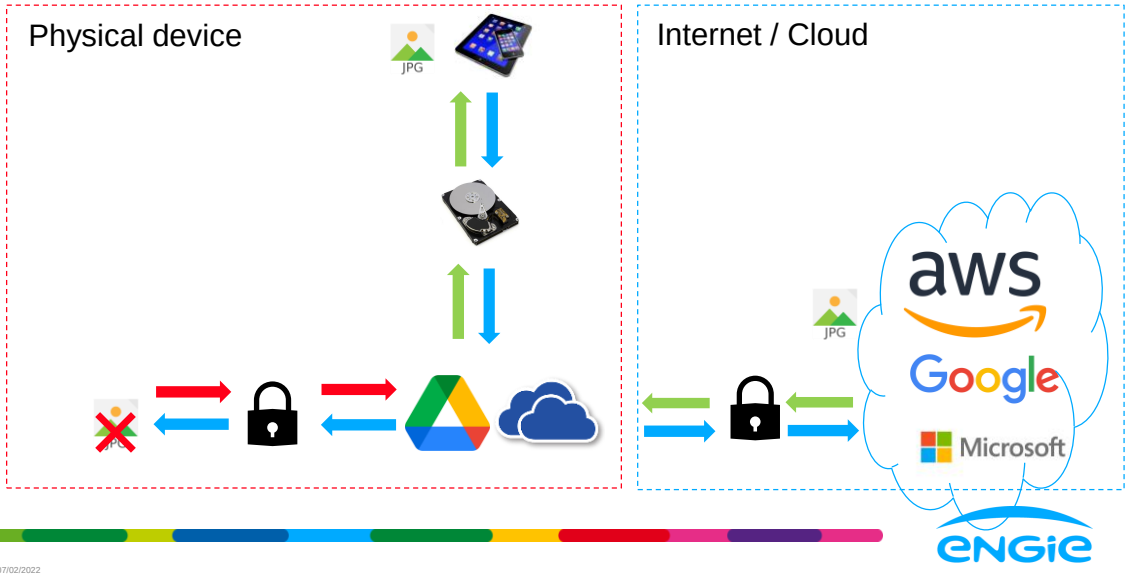






42

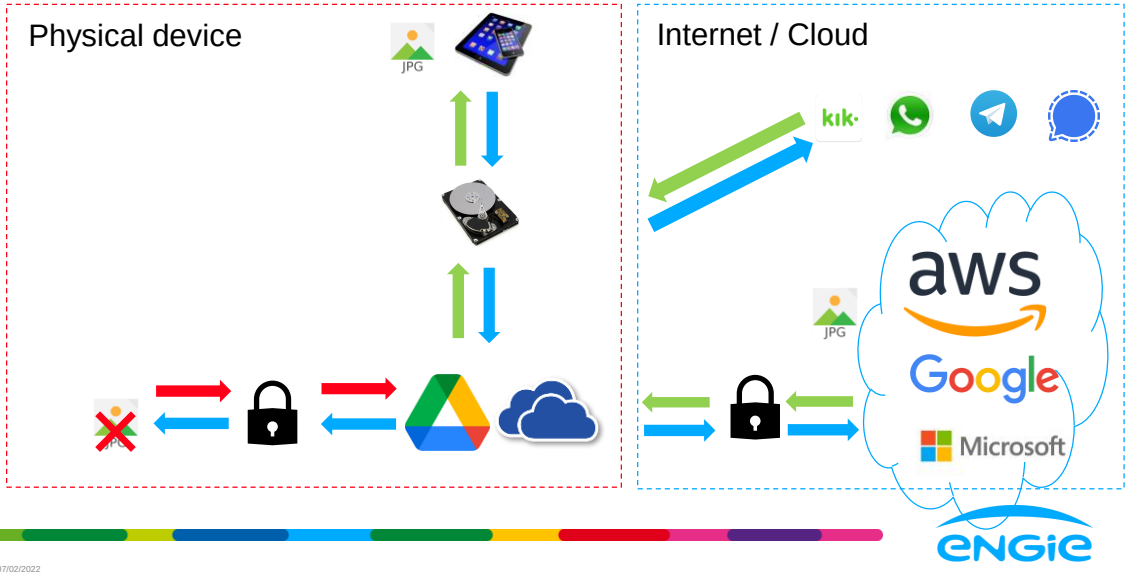
# Physical to Logical




43 07/02/2022

43

# Physical to Logical

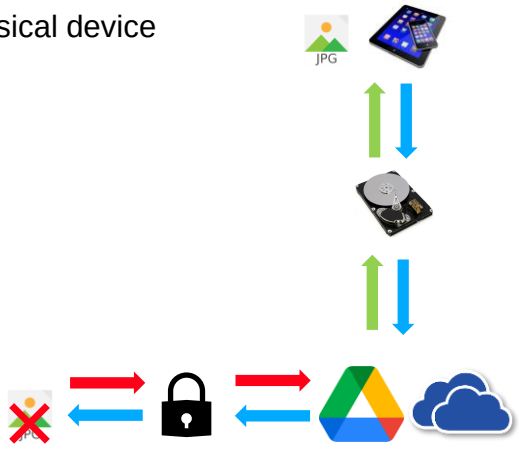



44 07/02/2022

44

# Physical to Logical

Physical device




Internet / Cloud


- Data is offent encrypted during transfer, but not always encrypted at rest.
- The location of the encryption keys may vary



45

# Extraction challanges

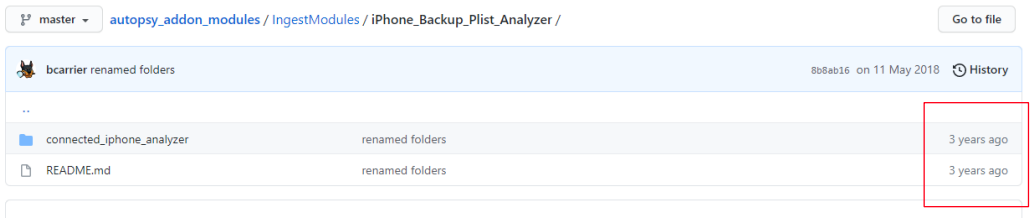
- Pythsical extractions are becoming a thing of the past. Data is often lost.
- While Open source tools exist for forensic analysis the development in the field is very fast.



46

# Extraction challanges

- Pythsical extractions are becoming a thing of the past. Data is often lost.
- While Open source tools exist for forensic analysis the development in the field is very fast.






47

# Extraction challanges

- Pythsical extractions are becoming a thing of the past. Data is often lost.
- While Open source tools exist for forensic analysis the development in the field is very fast.
- Are we allowed to connect to the cloud to retive the data not on the device?



48

# Summary

- When handeling mobile devices access to the pythsical storage is restricted
- Encryption added aditional layers or virtual access
- Data location is not always known by the user.
- Data is presented in a uiform way to the user.



49


50

# Electronic evidence and criminal procedure.

## From open source to dark web.

ENELI LAURITS

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

1



## Setting the stage

1. Using electronic evidence in court. Some possible issues that could be raised, evidentiary objections.
2. How to collect electronic evidence ***according to law***?
3. Publicly available data and social media. Reasonable expectation of privacy and restrictions to collection of evidence.
4. Dark web?

2

# Electronic evidence in court proceedings

- As far as the applicable law allows for it, and subject to the court's discretion, the acceptance as evidence of all types of electronic evidence is encouraged and recommended for court practice.
- If there is a dispute, the parties generally identify the issues to be resolved, and unless a party raises the issue of the authenticity of the electronic evidence, the court does not need to raise the issue on its own initiative.
- The party seeking to rely on electronic evidence may be required to demonstrate its authenticity.

3

SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

# Electronic evidence in court proceedings

- Evidence is generally admissable almost automatically as long as no party objects its admissal.
- Digital evidence must be obtained in compliance with existing legislation and best practices to be admissible in court.
- Any piece of digital evidence should be complete and tell the whole story.
- Digital evidence must be collected, handled and analysed in a way which does not cause doubt about its veracity.
- Digital evidence must be believable and understandable to a judge.

4

# Evidentiary objections

- **The identity of the author may be in dispute (SODDI).**

Evidentiary goal:

- Prove the identity using circumstantial evidence.

- **It may be claimed that the records were altered, manipulated, or damaged between the time they were created and the time they appear in court as evidence.**

Evidentiary goal:

- Prove that digital evidence is authentic, complete and reliable.

5



# Evidentiary objections

- **The reliability of the computer program that generated the record may be questioned.**

Evidentiary goal:

- Prove that computer program was working as intended and show its function.

- **It may be claimed that malware was the source of problems/records.**

Evidentiary goal:

- Prove that mentioned malware does not work the way described or prove absence of malware.

6

# Requirements for admissibility - legitimacy

Digital evidence is considered legitimate and lawful when:

- It has been gathered without violating fundamental rights.
- It has been obtained and processed according to the procedure established by law.

7



# Capturing evidence from the internet

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

A Party may, without the authorization of another Party:

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

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

8

# What to keep in mind

Digital evidence:

- Is latent, like fingerprints or DNA evidence;
- Crosses jurisdictional borders quickly and easily;
- Is easily altered, damaged, or destroyed;
- Can be time sensitive.

- Which issues might this raise in courts?

9



# Collection – need for procedural rules?

- The principles of computer-based electronic evidence (ACPO Guidlines):

**Principle 1:**

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.

10

# Collection – need for procedural rules?

The principles of computer-based electronic evidence.

**Principle 2:**

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.

11



# Collection – need for procedural rules?

The principles of computer-based electronic evidence.

**Principle 3:**

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.

12

# Collection – need for procedural rules?

The principles of computer-based electronic evidence.

**Principle 4:**

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

13



# Capturing evidence from the internet

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

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

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

14

# US v Auernheimer

The defendant was convicted of unauthorised access for collecting information from a website of US telecommunication provider which was accessible on a hard to guess website that was not intended to be accessed.

Although the data was publicly accessible the court stated that analogous to a home where 'the front door is left open or unlocked' the data was still protected.

The defense argued that the information was made available to everyone and the general public was authorised to view the information.

15



# Social media evidence – publicly available?

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

16

# Social media evidence – privacy concerns

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

17



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

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

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

The public availability for such restricted data hence often depends on factual barriers that these settings eventually raise. Data on social networks are easily relatable to natural persons and often give insights in particularly sensitive areas of a persons' life such as religious or political beliefs or sexual preferences. Accessing social media data is hence bears severe risks to the fundamental rights of the data subject. While data on social media may be manifestly made public, this cannot be re-interpreted as consent or abandoning fundamental rights protection.“

18

# United States v. Meregildo

Government's method of collecting evidence was challenged, that is Government's use of a cooperating witness who was one of suspect's Facebook "friends" and gave the Government access to suspect's Facebook profile.

To which extent can one say that his social media account is private? Could it be at some circumstances be seen as publicly available information? Could LEA collect such data without any further authorisation?

19



- Where Facebook privacy settings allow viewership of postings by "friends," could the Government access them through a cooperating witness who is a "friend" without violating the rights for privacy?
- While user undoubtedly believe that his Facebook profile would not be shared with law enforcement, does he have justifiable expectation that his "friends" would keep his profile private? And the wider his circle of "friends," the more likely his posts would be viewed by someone he never expected to see them.
- User's legitimate expectation of privacy ends when he disseminates posts to his "friends" because those "friends" are free to use the information however they want—including sharing it with the Government.
- The argument that the user with a private setting has a reasonable expectation of privacy because he had a limited number of followers has nothing to do with his attempts to keep his messages private.

20

# Social media evidence

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

**Methods of authentication include:**

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

21



# Social media evidence

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

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

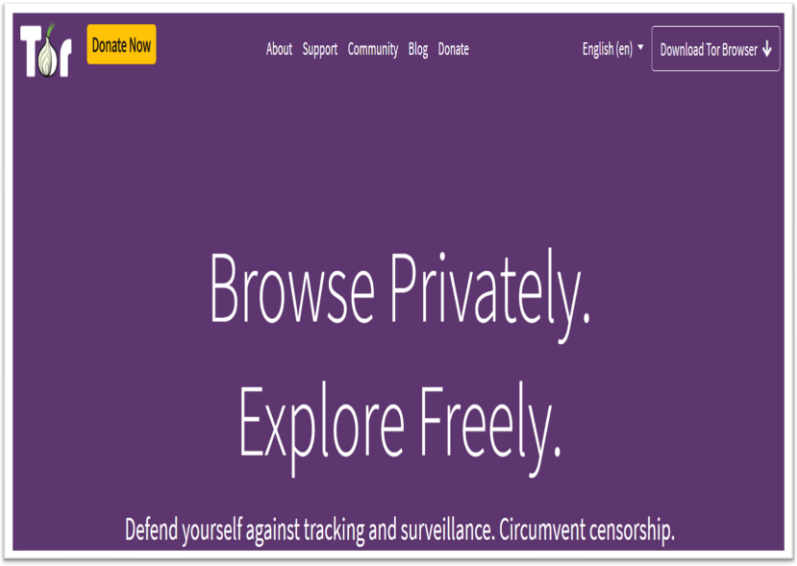
Testimony by a witness who viewed the information on the website is usually sufficient to meet the latter requirement.

22

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

23






The dark web is a part of the internet that isn't indexed by search engines.

It forms a small part of the deep web.

Darknet websites are accessible only through networks such as Tor.

24

# Tor

- Tor (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption.
- Tor makes it very difficult to physically locate computers hosting or accessing websites on the network.
- This difficulty can be exacerbated by use of additional tumblers or anonymisers on the Tor network.
- Tor is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity.

25



# Capturing evidence with surveillance methods

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

26

# Capturing evidence with surveillance methods

- The term “network investigative technique” is a euphemism for law enforcement hacking;
- it describes a law enforcement surveillance method that entails remotely accessing and installing malware on a computer without the permission of its owner or operator.
- Network investigative techniques are especially useful in the pursuit of criminal suspects who use anonymizing software to obscure their location.

- NITs have lead to many cases which have eventually ended up in international cooperation. As Kerr and Murphy* put it: „To date, not only has the most usual response [to discovering a foreign law enforcement agency engaged in the unauthorised access of data stored within its jurisdiction] been one of acquiescence, but, indeed, of providing even more cooperation.“

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

27



# Evidence collected in the dark web?

- Turn to slides 3 ja 4, but most importantly:
  - Evidence is generally admissable almost automatically as long as no party objects its admissal.
  - Digital evidence must be obtained in compliance with existing legislation and best practices to be admissible in court.
  - As Kerr and Murphy argue:

*„When a widespread practice by states exists, either in the form of active practice or in the form of acquiescence to the practice of others, undertaken in a belief that the practice is lawful (referred to as opinio juris), then a rule forms around that practice.“*

28

THANK YOU!

29

ERA 2022

# CHALLENGES RELATED TO INVESTIGATION AND COLLECTION OF E-EVIDENCE

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

1

## Danijel Sladović

- Consultant at INsig2, Department of Digital forensics
  - Training, conducting investigations, consultant for clients
- Studied at Faculty of Organization and Informatics
  - Masters degree
- Over 4y of experience in Digital forensics
- Certificates: CEH, Blackbag, Magnet, Belkasoft…
- Specialist in Linux, MacOS, Network, Internet forensics, Python, Live data, Car, computer HW…

www.insig2.com
DanijelS@insig2.com

2

# INsig2 Trainings

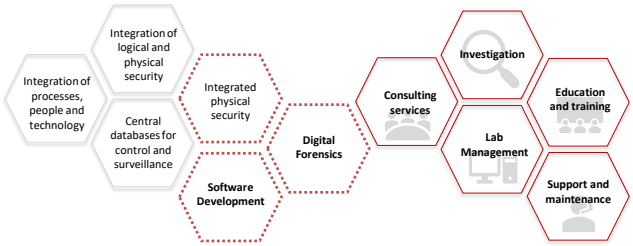
- Intensive training schedule has been in place since late 2011 and since then INsig2 successfully completed over 200 trainings at 4 continents and trained over 4000 law enforcement professionals






# What do we do?

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



# INsig2 projects & references


European Digital Forensics Training,
4 years contract


Sophisticated security systems


Development of sophisticated security systems


Microsoft Global Security Partner for CEE

Sectors served:

- Pharma
- Defence
- Ministries
- Software
- Steel
- Telecomm
- Law enforcement
- Banks
- Airports
- Retail

INSIG2

5

5

# Cars as a source of e-evidence

INSIG2

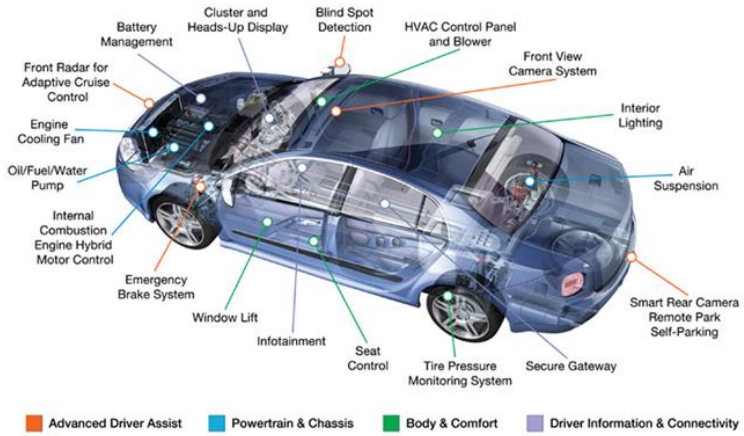
6

# CAR CONNECTIVITY

- Bluetooth
  - Connection to infotainment in car
  - Make a call
- Wi-Fi
  - To connect to an access point
  - To share Wi-Fi to the vehicle
- Using 3G, 4G and 5G networks
  - To update vehicle software
  - To connect with Internet
- Tethering (phone-as-modem)
  - Instant in-car hotspot

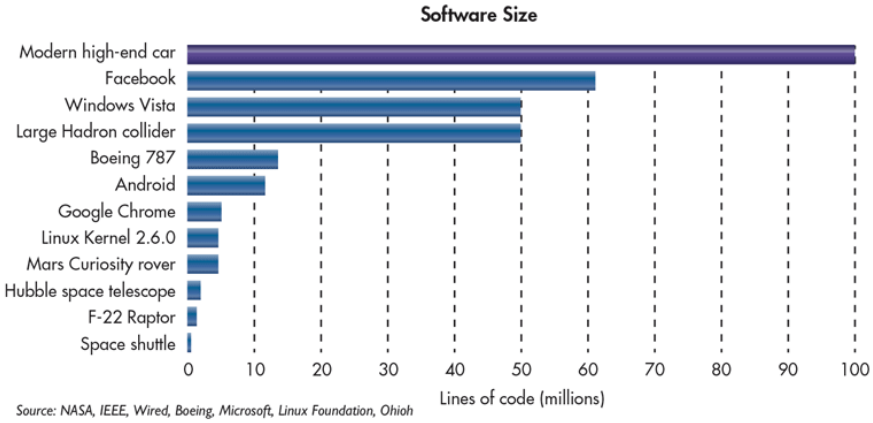

7

# SYSTEMS INSIDE VEHICLES




8

# VEHICLE SYSTEM - SOFTWARE




9

# CRASH DATA RETRIEVAL

- Extraction of data from “Black Boxes” or ECU’s directly
- Forensically sound
  - Pre-crash speed
  - Braking
  - Seatbelt usage
  - Airbag deployment
  - Steering
  - Throttle position
  - Delta-V (change in velocity)
  - Only 2-5 seconds prior to crash
  - Specific Black boxes provided by insurance companies
    - Can hold data for few weeks (depends of policy)

10

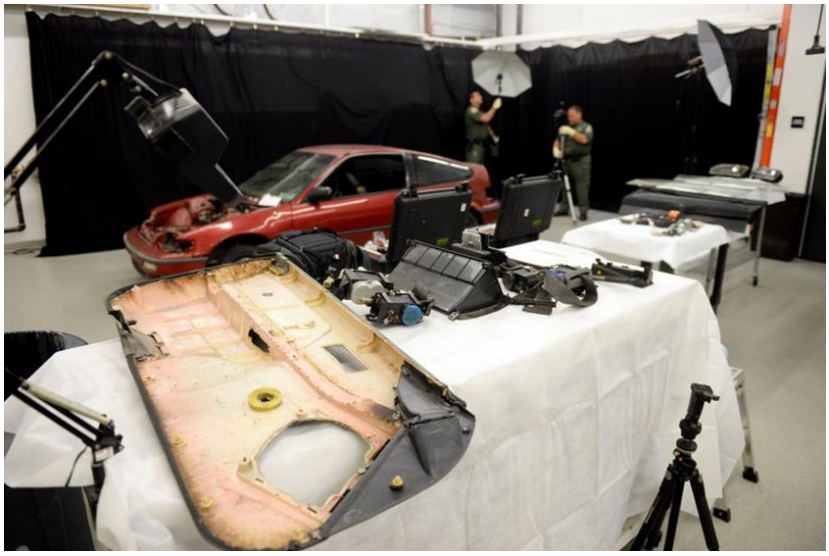
# CAR FORENSICS

- Extraction of data from ECU's (Infotainment)
- Forensically sound
  - Speed
  - Seatbelt usage
  - Airbag deployment
  - Using of mobile phones while driving
  - Driver distractions (speed warnings, etc.)
  - Driver habits (constant hard acceleration, hard braking, fast driving, etc.)
  - Locations

INSIG2

11

# WHAT CAR FORENSICS LOOKS LIKE



INSIG2

12

## Android Auto & Apple CarPlay

- Not a real infotainment system
- Third party app that mimic the functions of your phone and run on vehicle computer interface
- Apple CarPlay
  - Connect your iPhone into car using USB
  - Phone, music, maps, messages, podcasts, audio, etc.
- Android Auto
  - Download an application and sync your phone with car
  - Recent activities, navigation, calls and messages

INSIG2

13

## DIGITAL EVIDENCE STORAGE MEDIA

- Flash memory
- SD cards
- PCMCIA Cards
- Hard drives

INSIG2

14

# KEY FOBS

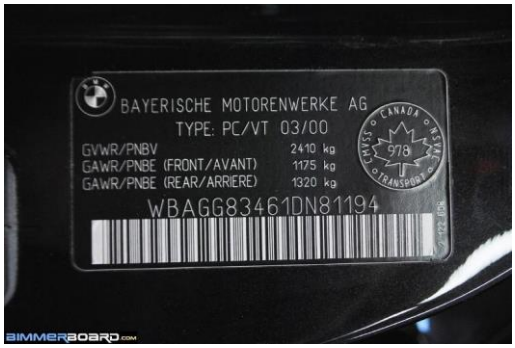
- BMW and Audi store the most user data in key fobs
- Stored info: Brand information, Transponder Type, Key ID, Key Type, Key Number, VIN, Key Status, Vehicle Mileage, Last Time in Vehicle, Fuel Level, Coolant Temperature, Outside temperature, Exterior Colour

| | | | |
|---|---|---|---|
| Fahrzeugidentnr. | WBAUC7C52AVK81387 | Fabrikat | BMW |
| Modell: | UC73 | Typschlüssel: | 135i N54 |
| Leittyp: | UC73 | Farbcode | 0354 |
| KM-Stand | 14.944 km | Einlesedatum: | 18.06.10 14:13 |
| Schlüssel - Variante: | 8 | Schlüssel - Subvariante | 8 |
| Polstercode | LWD1 | Herkunft | K |
| Letzte Aktualisierung | 18.06.10 14:08 | Produktionsdatum | |
| Herstellungsdatum | 01.2010 | Erstzulassung: | 23.01.10 |
| § HU | 01.01.13 | § AU | 01.01.13 |
| Bremsflüssigkeit | 01.01.12 | Tankinhalt | 44 Liter |
| Kühlmittel Temp. | 96 °C | Aussentemperatur. | 14,5 °C |
| Durchschnittliche Laufleistung (km/Woche) | 320 km / Woche | Restweg | |
| Nächster Service | 34.000 km | Service LEDs | |
| Code für die fällige Serviceart | Unbekannter Fehler | Erweiterte Schlusselattribute | |
| iLevelPlant | E89X-09-12-512 | newILevelAvailable | true |
| keyNumber | 1 | keyProfil | 1 |

15

# DIGITAL EVIDENCE FROM CAR

- Vehicle/System Information
  - Serial number of System
  - Part numbers
  - Original VIN number
  - Build Number




16

# DIGITAL EVIDENCE FROM CAR

- Installed Application Data
  - Weather
  - Traffic
  - Facebook
  - Twitter
  - Emails
  - Credentials


17

# DIGITAL EVIDENCE FROM CAR

- Connected Devices
  - Phones
  - Media Players
  - USB Drives
  - SD Cards
  - Wireless Access Points
  - Bluetooth AP

18

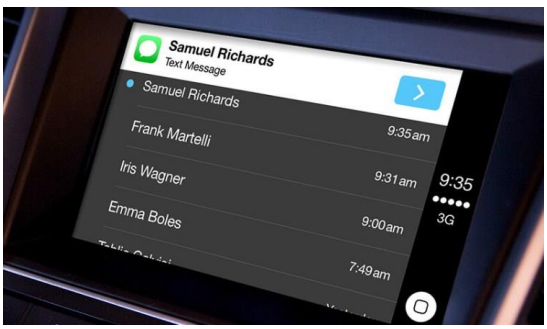
# DIGITAL EVIDENCE FROM CAR

- Navigation Data
  - Tracklogs and Trackpoints
  - Saved Locations
  - Previous Destinations
  - Active and Inactive Routes


19

# DIGITAL EVIDENCE FROM CAR

- Device Information
  - Device Ids
  - Calls
  - Contacts
  - SMS
  - Audio
  - Video
  - Images
  - Access Point Information
  - MAC addresses




20

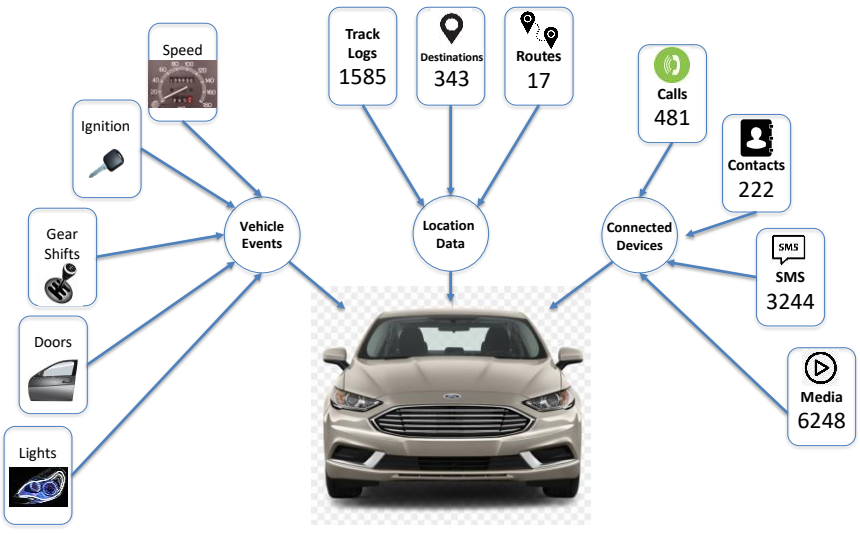
# DIGITAL EVIDENCE FROM CAR

- Events
  - Doors Opening/Closing
  - Lights On/Off
  - Bluetooth Connections
  - Wi-Fi Connections
  - USB Connections
  - System Reboots
  - GPS Time Syncs
  - Odometer Readings
  - Gear Indications

INSIG2

21

# VEHICLE DATA CAN BE USED AS KEY EVIDENCE




INSIG2

22

## Gathering data from IoT devices

23

## Apple Watch forensics

- Ways of acquiring data from Apple Watches:
  - Backup of the synced iPhone (iCloud/iTunes)
  - Device
  - Cloud (synced health data)

24

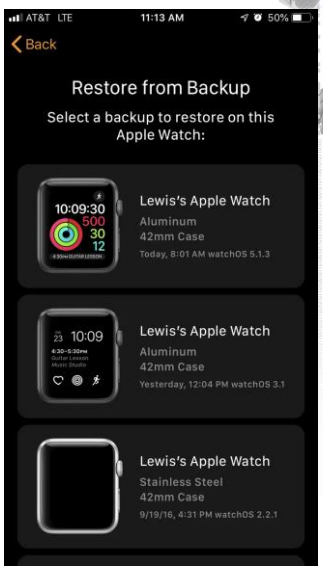
# Apple Watch backup

- Apple Watches don’t have any backup services running on the watchOS
- The Apple Watch automatically creates a backup on the paired iPhone when:
  - the watch is unpaired from the iPhone
  - when the user pairs a new phone to a watch
  - When watch is out of range from the paired iPhone

25

# Apple Watch backup

- The list of watch backups that can be restored will be available on the user's iPhone/watch app
- On restore the watch version should match
- Some information can be visible in the iPhone settings (General/iPhoneStorage/Watch)
- The backups can't be changed or acquired from watch app
- Backups can't be deleted separately; deletion is only possible if all backups are deleted




26

## Apple Watch backup: What is inside?

- Built-in app data and settings
- Setting for third-party apps
- App layout on Home screen
- Clock face and dock settings
- Notification settings
- Playlists, albums and mixes
- Siri voice feedback settings
- Time zone

- Health and fitness data:
  - History
  - Achievements
  - Workout and activity
  - Calibration data
  - User entered data

- The health backups can be recovered by using iCloud or an encrypted iTunes backup

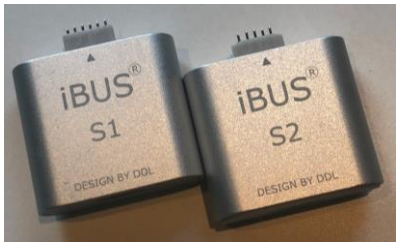
27

## Backup extraction

- If there is no backup created the watch must be unpaired to create a backup
- Investigator must obtain the iPhone that was connected to the watch
- The easiest way of extracting the backup is to connect the iPhone to iTunes and to create an encrypted backup
- Password protected backups contain more data than regular backups

28

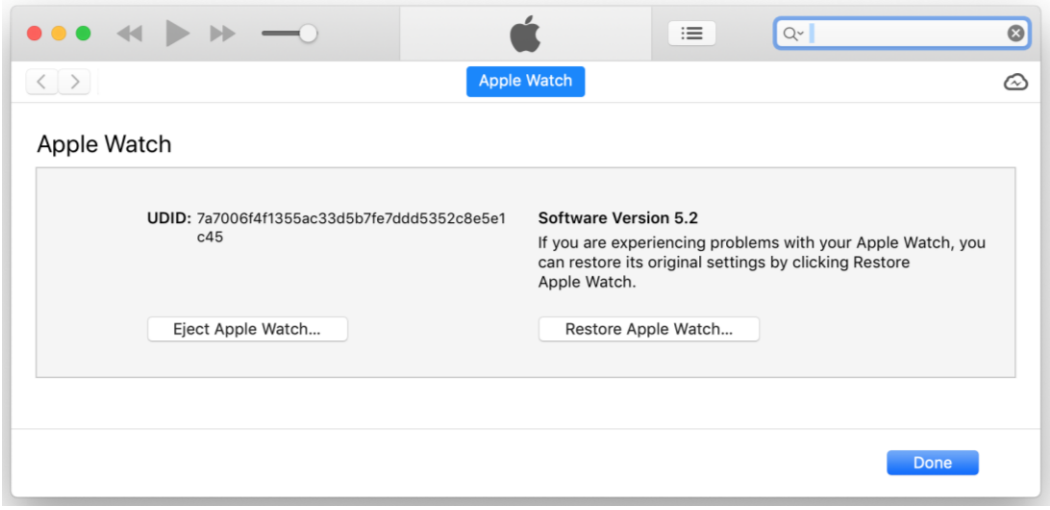
# Apple Watch IBUS acquisition






29

# Apple Watch IBUS acquisition




30

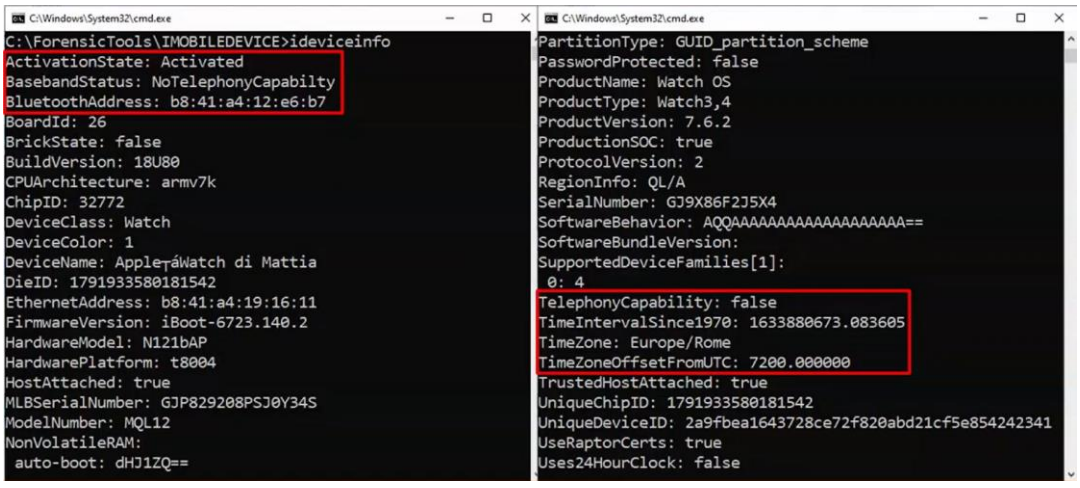
# Apple watch acquisition option

- Full file system acquisition might be possible using jailbreak
  - jelbrekTime watchOS 4.1
  - Brenbreak wathcOS 4.0-5.1.2
  - Chakra1n (based on checkm8 exploit)
- Forensic tools for iPhone devices
- AFC (Apple File Conduit) is the only reliable method that can extract:
  - media files
  - comprehensive information about the device
    - serial numbers
    - Bluetooth ID
    - Wi-Fi ID
  - Log files

INSIG2

31

# Extracting basic device information

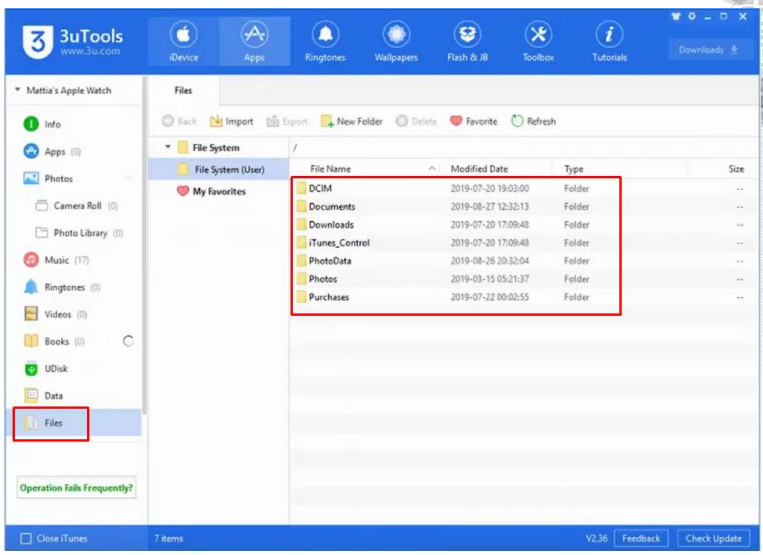



INSIG2

32

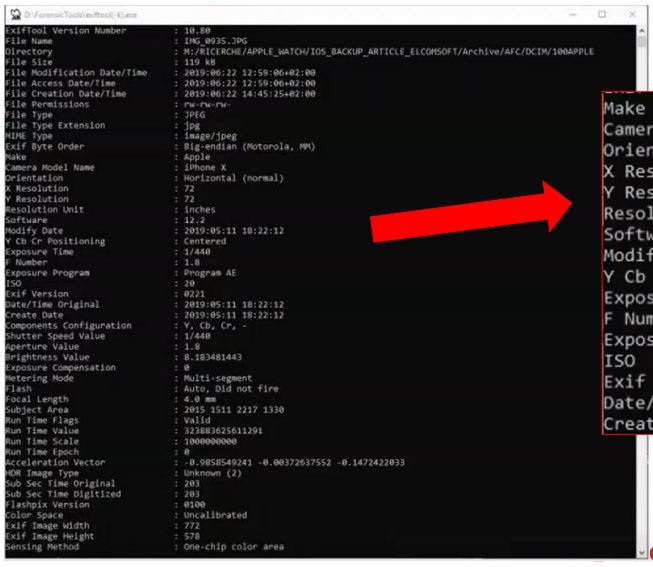
# Extracting basic device information

- By using forensic tools, we can access specific folders from the watch by using AFC




33

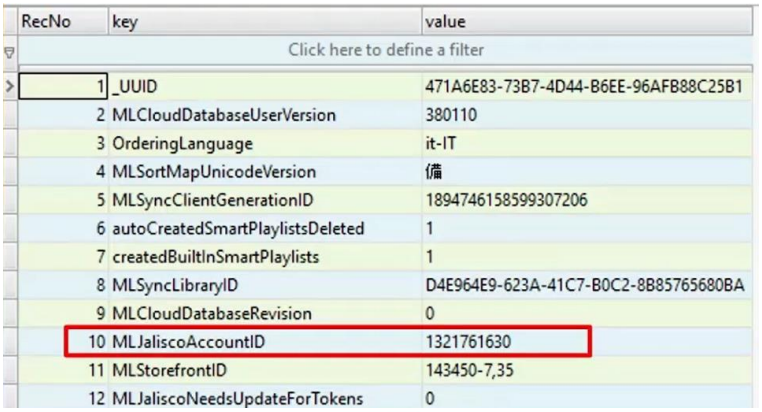
# Extracting basic device information




34

# Apple watch – iTunes directory

- Important database that can be found in iTunes library folder is called "MEDIALIBRARY.SQLLITEDB"



| RecNo | key | value |
|---|---|---|
| Click here to define a filter | | |
| 1 | _UUID | 471A6E83-73B7-4D44-B6EE-96AFB88C25B1 |
| 2 | MLCloudDatabaseUserVersion | 380110 |
| 3 | OrderingLanguage | it-IT |
| 4 | MLSortMapUnicodeVersion | 備 |
| 5 | MLSyncClientGenerationID | 1894746158599307206 |
| 6 | autoCreatedSmartPlaylistsDeleted | 1 |
| 7 | createdBuiltInSmartPlaylists | 1 |
| 8 | MLSyncLibraryID | D4E964E9-623A-41C7-B0C2-8B85765680BA |
| 9 | MLCloudDatabaseRevision | 0 |
| 10 | MLJaliscoAccountID | 1321761630 |
| 11 | MLStorefrontID | 143450-7,35 |
| 12 | MLJaliscoNeedsUpdateForTokens | 0 |

35

# Apple TV data acquisition

- Apple TV does not have backup services
- No password protection
- Possible acquisitions:
  - Device information and list of installed programs
  - AFC (Apple File Conduit)
  - Crash logs
- Full file system can be acquired by using :
  - Uncover 5.3.0 tool
  - Checkra1n jailbreak (Apple TV 4)

36

## Apple TV data acquisition

- Different from Apple Watch, Apple TV can have a CPL (Cloud Photo Library) folder if enabled from the user
- If file system is acquired different user activity information can be found:
  - Headboard information (pictures, icons for all the applications that the user had installed with the timestamps)
  - Cashed data
  - User movie history
  - Cashed streamed file
  - Data from apps installed on Apple TV
  - etc.

37

## Investigating the Dark Web

38

## Dark Web

- Dark web is the part of internet that consists of hidden services
- Dark web can be accessed using specific software that:
  - Has a specific configuration
  - Has authorization to access
- The content of the dark web doesn't appear on the surface web or Internet
- The contents of the dark web can't be indexed by regular search engines

39

## Dark Web


40

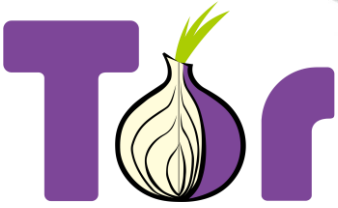
## Who created the dark web ?

- Dark Web really got its start in March of 2000 with the release of Freenet
- Freenet is one of the earliest darknets
- It was created at the University of Edinburgh and was based on a student research paper written in 1999 by Ian Clark
- The goal of Freenet is to create an encrypted network that resists censorship
- Most important Dark Web development happened in 2002, with the release of TOR or The Onion Router, created by the United States (US) military to help their own operatives remain untraceable

INSIG2

41

## Tor Browser



- Tor is an open-source browser based on Firefox
  - Tor is an acronymous for “The Onion Router”
  - https://www.torproject.org/download/
- Enables anonymous communication
- Tor is used to direct internet traffic through a free worldwide, volunteer overlay network
  - Tor network consists of more than seven thousand relays
  - The network conceals user location and internet activity (prevents network surveillance)

INSIG2

42

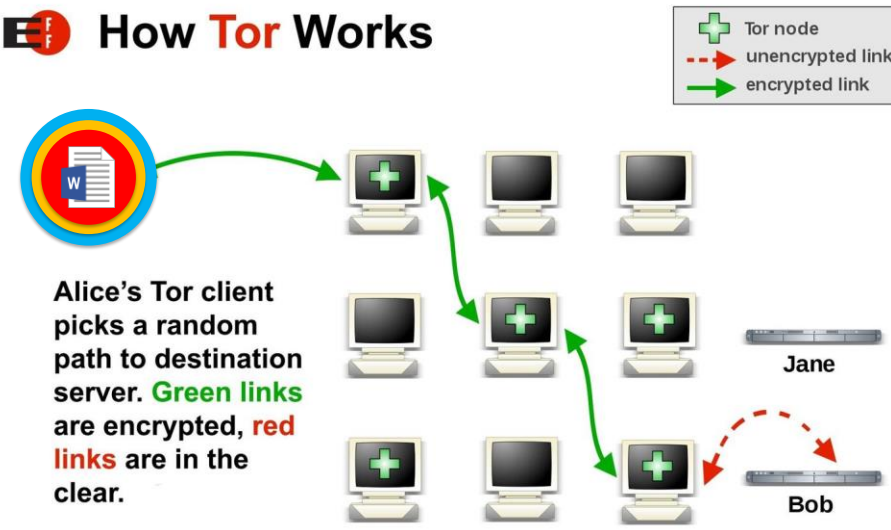
# TOR ("The Onion Routing")

- Onion routing was developed by the US Navy
  - To protect US intelligence communications online
  - Later made open source
- Data is encrypted multiple times and transmitted through nodes called onion relays/routers
  - **Direct link is broken**
    - Data is bounced between multiple relays (~7000)
- **Onion Service Protocol** ("hidden services")
  - Users can hide their location while offering various kinds of services

INSIG2

43

# How Tor Works




INSIG2

44

## Dark Web usage

- Military, government, and law enforcement organizations
  - Confidential emails
- Popular in countries with censorship and political imprisonment
  - Freedom from potential oppression and monitoring
- Journalists and whistle-blowers
  - Exchange sensitive information
  - Protect research and sources

45

## Dark Web usage

- Home users to protect themselves when online
- Terrorists also use it for the same reasons, and so do the Dark Web's most publicized users—***criminals***

- **Marketplaces with illicit goods**
  - Narcotics
  - Firearms
  - Counterfeit
  - Stolen credit cards
  - Ransomware


46

## Cryptocurrencies in Dark Web

- Cryptocurrencies made it possible to conduct business transactions anonymously
  - **Allows users to engage in illegal activity**
- Bitcoin, Litcoin, Peercoin, Primecoin, Ripple…


47

## Challenges

- Legality
  - All the components used by dark web markets (Tor, Bitcoin, VPN) — legal
- Jurisdiction
  - Servers can be anywhere in the world
- Skill set
  - Dark web, Tor, Cryptocurrency, Encryption…

48

## Using virtualization of evidence for investigators

49

## Image virtualization

- Used to mount the contents of disk images as complete disks in Windows
- Can benefit the investigator to see disk-specific features, like integration with Disk Manager
- Most of the forensic image mounter tools features that allow investigators to:
  - bypass Windows authentication
  - managing Bit-Locker protected volumes
  - mounting shadow copies
  - Built-in write-blocking

50

# Image virtualization tools

- Some of the popular forensic virtualization tools are:
  - Sumuri Carbon
  - Arsenal Image Mounter
  - Access Data - FTK Imager (enables mounting of disk partitions)

CARBON
VIRTUAL FORENSIC SUITE

ARSENAL RECON

INSIG2

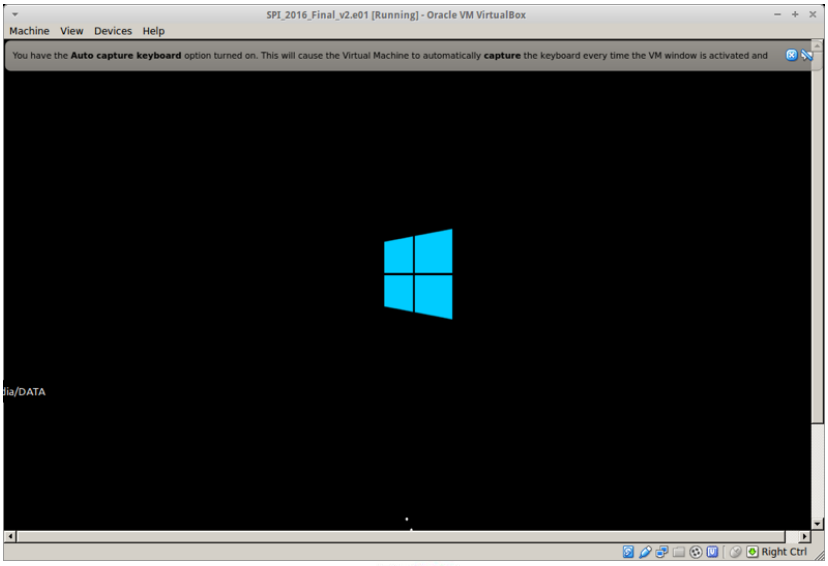
51

# Sumuri Carbon virtualization


INSIG2

52

# Sumuri Carbon virtualization




INSIG2

53

# Thank you!


danijel.sladovic@insig2.com

INSIG2

54

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



2

## Guideline

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



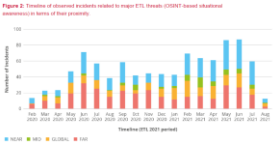
3



## We are under attack

Cybercriminals are increasing efficiency with coordinated attacks

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

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

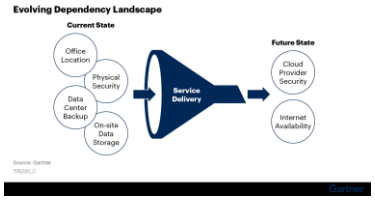
- January: Microsoft Exchange Server data breach
- April: Over 500 million Facebook users' personal info was discovered posted on a hackers' website
- April: The Ivanti Pulse Connect Secure data breach of unauthorized access to the networks
- May: Operation of the U.S. Colonial Pipeline is interrupted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

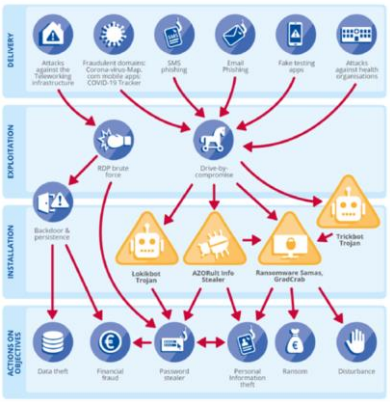


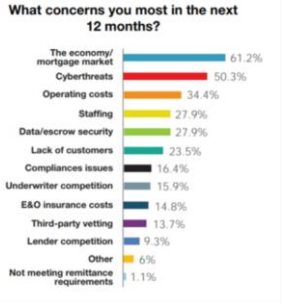
4

## Near future, post Covid 19

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










## Developments



## Achievements

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

## Mutual Legal Assistance

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

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

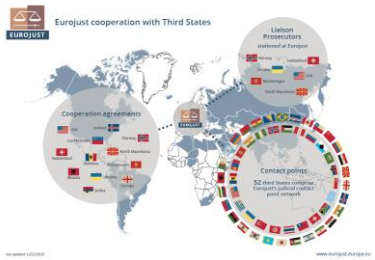






## General Principles International Cooperation in Criminal Matters

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



## Difficulties traditional MLA in cybercrime cases

- Traditional legal concepts
- Territoriality
- Jurisdiction


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







## European Production and Preservation Orders
### Background

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

**First**

Digital evidence is held on servers owned by service providers.

**Second**

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

## European Production and Preservation Orders
**Summary of the proposed Regulation**

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



11



## European Production and Preservation Orders
**Legal Basis, Subsidiarity and Proportionality**

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




12

## 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.







## Case Study

de Rechtspraak
Rechtbank Zeeland – West-Brabant

**Thanks!**

**Questions?**

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

15

Hessisches Ministerium der Justiz

HESSEN

# Special investigation techniques: A new evidentiary frontier for prosecutors

## OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

**Thessaloniki**
**7 - 8 February 2022**

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

Hessisches Ministerium der Justiz

HESSEN

## Encryption is an enabler for OCGs


### Welcome to the Evolution

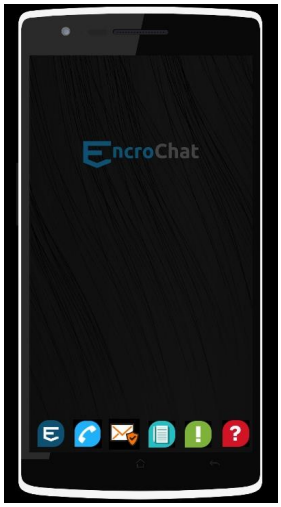
EncroChat is an end-to end security solution, not just another downloadable 'secure' software application.

Individual software applications cannot isolate themselves from other installed software applications, the operating system the device relies on, or the network they connect to. The integrity of the solution is paramount. This includes securing the hardware, operating system, software applications, data transit, network infrastructure and servers. Ignoring any facet of this is devastating and renders the actual security of the product to the level of marketing hype.

EncroChat protects conversations with the following four tenets

- **Perfect Forward Secrecy** Each message session with each contact is encrypted with a different set of keys. If any given key is ever compromised, it will never result in the compromise of previously transmitted messages – or even passive observation of future messages.
- **Repudiable Authentication** Messages do not employ digital signatures that provide third party proofs. However, you are still assured you are messaging with whom you think you are.
- **Deniability** Anyone can forge messages after a conversation is complete to make them look like they came from you. However, during a conversation

# The Encrochat investigation




- **GUARANTEED ANONYMITY - No way to associate device or SIM card to customer account**
- **CUSTOMISED ANDROID PLATFORM Fully encrypted from power on. Focus on security and privacy. Simplified user settings.**
- **DUAL OPERATING SYSTEM Subscribers can now launch either a standard Android OS or the EncroChat OS. Two distinctive Operating Systems packaged with each device.**
- **MESSAGING PROTOCOL The electronic equivalent of a regular conversation between two people in an empty room.**
- **MESSAGES THAT SELF-DESTRUCT With our advanced burn a user can force wipe their own messages from another user's device using a timer countdown.**
- **PANIC WIPE From screen lock a user can type in a PIN and instantly wipe device's data.**
- **PASSWORD WIPE After a set amount of password attempts on device all data is wiped.**
- **SECURE BOOT Upon boot, the device internally checks itself to ensure no one has tampered with the system files.**





# The Encrochat investigation

- "EncroChat" was a provider of cell phones on which an app was installed that allowed EncroChat users to send encrypted messages to each other.
- Due to the specifics of the system, the distribution channels, and the high cost of such a device, EncroChat phones were and are believed to be used almost exclusively for conducting criminal business.
- In 2020, a JIT of French and Dutch investigators succeeded in securing messages and images exchanged via the EncroChat server in unencrypted form.

## The dismantling of an encrypted phone solution used by organised crime groups

(source: https://www.eurojust.europa.eu/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe)

**Interception and analysis of millions of messages exchanged between criminals planning serious criminal acts**

This intensive operation informed hundreds of ongoing investigations, providing insights and access to new evidence to tackle international criminal networks involved in drug smuggling, money laundering and other forms of serious and violent crime, including murder, extortion, robbery, grievous assault and hostage taking.

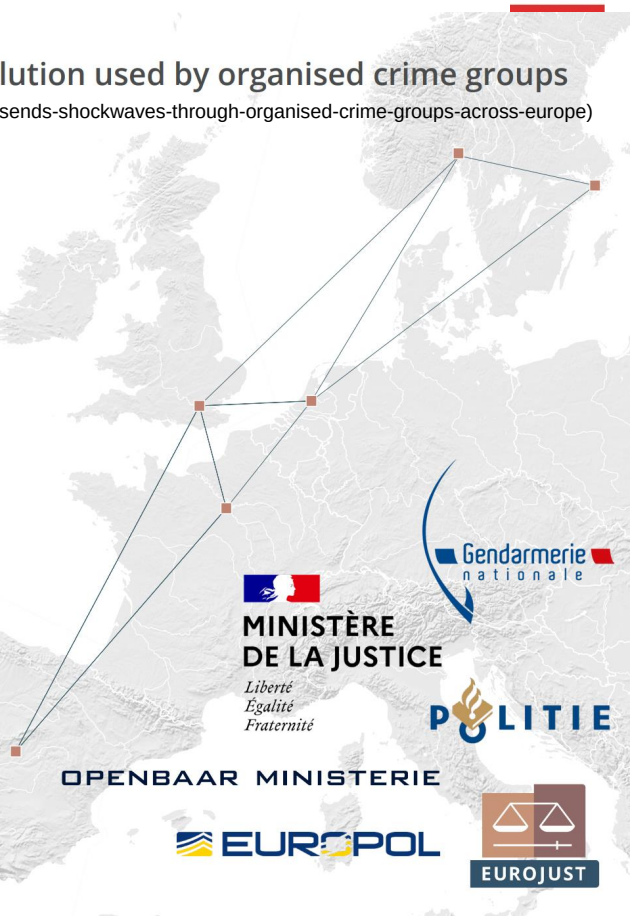
Intensive analysis was undertaken by Europol.

**Five coordination meetings** were held at Eurojust, with the active participation of national police forces and Europol to ensure smooth communication and coordination between all parties to the JIT. Two of these meetings also involved other countries, including Spain, Sweden, the UK and Norway. **Daily coordination meetings** between involved law enforcement partners were held at Europol.

A **joint investigation team (JIT) agreement** was signed between the national police and judicial authorities of France and the Netherlands in April 2020, supported by the French and Dutch Desks at Eurojust and by Europol.

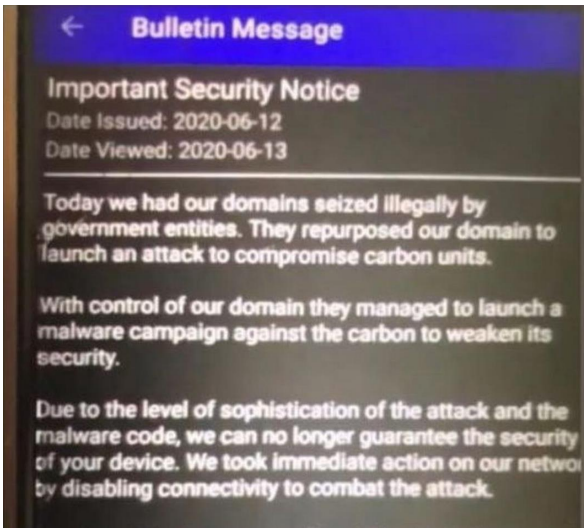
The case was opened by the French Desk and brought to the Dutch Desk at Eurojust in April 2019.

In 2017, **French police and judicial authorities began investigating** phones using the secured communication tool *EncroChat*, an encrypted phone solution widely used by criminal networks across the globe.






# The Encrochat investigation




- During the night of June 12 to 13, 2020, EncroChat issued a security alert to its customers, indicating that the solution was the victim of an "illegal seizure" by "government entities".
- They were advised to physically dispose of their device ("You are advised to power off and physically dispose your device immediatly").

HESSEN

# The Encrochat investigation


Hessisches Ministerium der Justiz

HESSEN

# The Encrochat investigation

- French investigative authorities have forwarded the data to many states outside the JIT, including Germany.
- In the course of evaluating the data, a large number of proceedings have been initiated throughout Germany or the data have been added to investigations already underway.
- Within these preliminary proceedings, the defense often doubts the admissibility of the data.

HESSEN

## Legal issues

- Different legislations have different rules on wiretapping / interception of telecommunications.
- In international transborder investigations, e.g. under the rules of an (EU) JIT, there might be legal options to share information gained through the interception of a telecommunication.
- Interception of TC vs. hidden search of the suspects data stored on mobile device: legal?
- Were the communications intercepted while they were being transmitted or while they were being stored in or by the system?





HESSEN

## Admissibility of the Encrochat evidence

- The decision of the Higher Regional Court of Bremen (handed down in December 2020) and the decision of the Higher Regional Court of Hamburg (handed down in January 2021) in two separate cases confirm that the collection of evidence by French authorities can also be used in German criminal proceedings if the interception of the surveillance reveals criminal activities from persons residing in Germany (in the cases at issue: drug trafficking offences).
- The information was lawfully made available to the German Federal Police Office via the exchange of spontaneous information and intelligence in accordance with Framework Decision 2006/960/JHA.

HESSEN

# Admissibility of the Encrochat evidence

1. The provision of Section 100e (6) No. 1 of the Code of Criminal Procedure, which is primarily designed for the exchange of data between different domestic criminal proceedings, is considered the legal basis for cross-border data traffic. The norm also permits the use of information from foreign criminal proceedings.
2. The use of the chat messages obtained, seized and evaluated by French investigative authorities in connection with the surveillance of the service provider for crypto cell phones (EncroChat) is not subject to any prohibition.
3. The necessary suspicion of crime is by no means based primarily on the use of effective encryption technology, as also offered by the leading messenger services, but primarily on the overall circumstances of the distribution and pricing of the EncroChat devices and the findings obtained in the French initial proceedings.
4. A possible violation of the duty to inform of the French investigating authorities according to Art. 31 para. 1 of the Directive does not lead to inadmissibility of evidence, if the German investigating authorities have made clear by their further conduct that they do not object to the investigative measures. This comes close to a subsequent cure of the violation.

Higher Regional Court Berlin, 30.08.2021 - 2 Ws 79/21, 2 Ws 93/21 – 161 AR 134/21





HESSEN

# Case Study: Operation Trojan Shield

***NEWS RELEASE***

***OFFICE OF THE UNITED STATES ATTORNEY***
***SOUTHERN DISTRICT OF CALIFORNIA***
***San Diego, California***

***Acting United States Attorney***
***Randy S. Grossman***

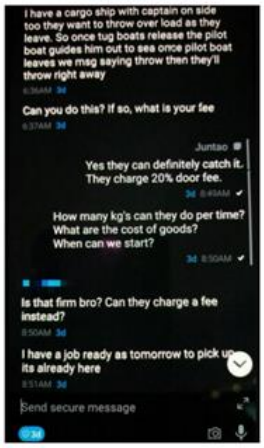
**For Further Information, Contact:**

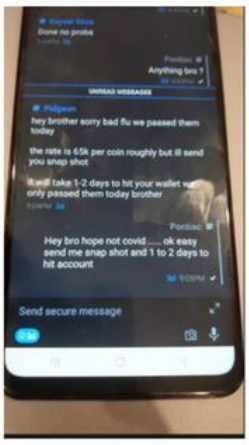
**Media Relations Director Kelly Thornton (619) 546-9726**

***For Immediate Release***

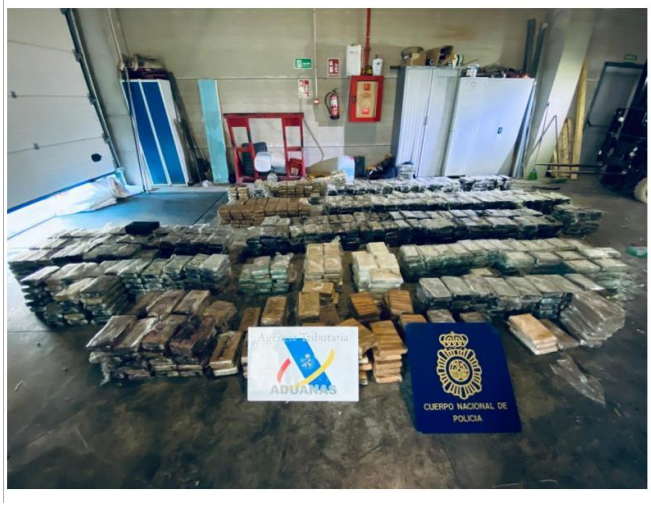
**FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown**


# Case Study: Operation Trojan Shield




hollowed out pineapples. The FBI and law enforcement officials in Spain reviewed the messages which contained specific details regarding the shipment and distribution once it arrived in Spain. The suspected container arrived into the Port of Algeciras, Spain on May 12, 2021. Law Enforcement officials in Spain conducted a search of the container and upon completion located approximately 1595 kilograms of cocaine.








# Case Study: Operation Trojan Shield

UNITED STATES DISTRICT COURT

unsealed on 6/7/21 per order -dlg

SEALED

for the

Southern District of California

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

Google LLC
1600 Amphitheater Parkway, Mountain View, CA 94043
Host of e[redacted]s@gmail.com

Case No. '21 MJ01948

**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 21 USC §§ 841, 846 | Conspiracy to Distribute Controlled Substances |

HESSEN

# Operation Trojan Shield

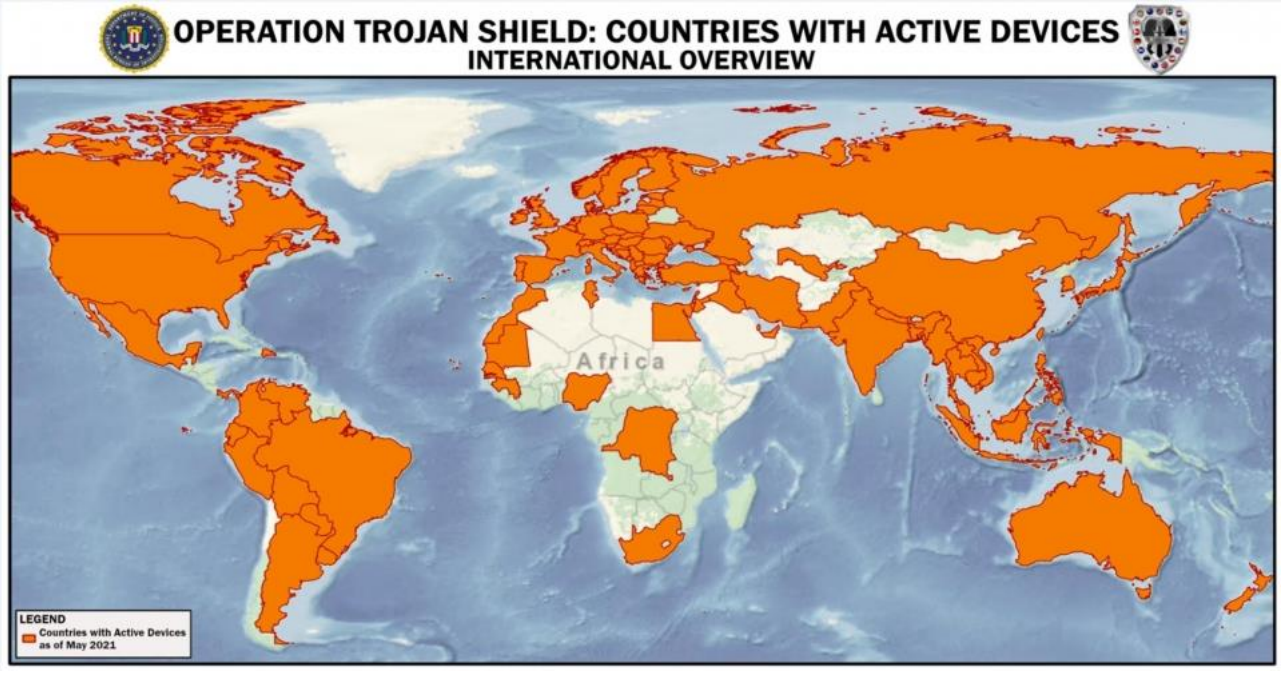
- The ANOM (also stylized as AN0M or ΛNØM) sting operation (known as Operation Trojan Shield or Operation Ironside) is a collaboration by law enforcement agencies from several countries, running between 2018 and 2021, that intercepted millions of messages sent through the supposedly secure smartphone-based messaging app ANOM.
- The ANOM service was widely used by criminals, but instead of providing secure communication, it was actually a trojan horse covertly distributed by the United States Federal Bureau of Investigation (FBI) and the Australian Federal Police (AFP), enabling them to monitor all communications.
- Through collaboration with other law enforcement agencies worldwide, the operation resulted in the arrest of over 800 suspects allegedly involved in criminal activity, in 16 countries.
- Among the arrested people were alleged members of Australian-based Italian mafia, Albanian organised crime, outlaw motorcycle clubs, drug syndicates and other organised crime groups.





HESSEN

# Case Study: Operation Trojan Shield



HESSEN

# Case Study: Operation Trojan Shield






HESSEN

# Admissibility of the ANOM evidence

1 HEs 427/21
62 Js 172/21 (ZIT)
9530 Js 217133/21
(StA Frankfurt am Main)

**OBERLANDESGERICHT FRANKFURT AM MAIN**

**BESCHLUSS**

“ (…) The defense's further statements that the authenticity of the data transmitted by the FBI cannot be verified and that there is a possibility of falsification of the contents, which is why they cannot be used, are also not convincing. The question of the authenticity of the data and the integrity of the data content, as well as what conclusions can be drawn from them, arises in the context of the evaluation of evidence, where the probative value is to be discussed. There is no comprehensive inadmissibility of the evidence in this respect. According to the current state of the investigation, there are no indications of manipulation of the data content or lack of authenticity. Rather, the mode of identification of the defendant only allows the conclusion that the defendant actually communicated with the co-defendants as documented under the nickname ‘XXX’. (…) “

Higher Regional Court Frankfurt/M, 22.11.2021 - 1 HEs 427/21

HESSEN

# Legal issues regarding cross border exchange of data

**COUNCIL FRAMEWORK DECISION 2006/960/JHA**

**of 18 December 2006**

*Article 7*

**Spontaneous exchange of information and intelligence**

1. Without prejudice to Article 10, the competent law enforcement authorities shall, without any prior request being necessary, provide to the competent law enforcement authorities of other Member States concerned information and intelligence in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA. The modalities of such spontaneous exchange shall be regulated by the national law of the Member States providing the information.

2. The provision of information and intelligence shall be limited to what is deemed relevant and necessary for the successful detection, prevention or investigation of the crime or criminal activity in question.





HESSEN

# Best practices

- Promoting effective cooperation, coordination, mutual legal assistance, and communication with relevant actors
- Allowing, where possible, alternatives to formal requests for mutual legal assistance
- Developing mechanisms for parallel or joint investigations
- Preserving the chain of custody and respecting the integrity of the criminal proceedings

HESSEN

# Information Sharing

*U.S. Department of Justice*
**Federal Bureau of Investigation**

**Precedence:** Routine
**Date:** [redacted]

Office of the Legal Attaché
United States Consulate
[redacted]

[redacted]

(U) UNLESS OTHERWISE PROVIDED HEREIN OR EXPRESSLY AUTHORIZED BY FEDERAL BUREAU OF INVESTIGATION (FBI) HEADQUARTERS IN A SEPARATE COMMUNICATION, THE INFORMATION IN THIS DOCUMENT IS FOR INTELLIGENCE AND LEAD PURPOSES ONLY, AND YOUR GOVERNMENT MAY NOT USE THE INFORMATION IN ANY LEGAL PROCEEDINGS, DISSEMINATE THE INFORMATION TO ANY OTHER GOVERNMENT, PERSON OR ENTITY, OR TAKE ANY OVERT INVESTIGATIVE STEPS (INCLUDING BUT NOT LIMITED TO FORMAL LEGAL PROCESS OR DIRECT CONTACT WITH REFERENCED PERSONS/ENTITIES OR THEIR ASSOCIATES) BASED ON THE INFORMATION IN THIS DOCUMENT.





HESSEN

# Handling Codes - Example

**SIENA H3 handling code for exchange of data within Eurojust case**

The provided data may be disclosed related to the XY investigations of the following countries:

Without prior permission from the providing authority you are not allowed to share this data with any other country.

In case the provided data leads to any entity in and/or link to the providing country, the providing authority would like to be informed as soon as possible.

The provided data can only be used for the purpose of the XY-investigations in the stated countries.

Upon finalization of the cases related to the XY-investigations, the provided data has to be destroyed at the earliest moment possible according to national law of the respective country, e. g. when the statute of limitations for criminal prosecution has come into effect or a conviction is final.

HESSEN

# Considerations for Electronic Evidence

**Admissibility**: Since the ultimate goal is the use of acquired and analysed evidence to support a case in court, electronic evidence must be obtained in compliance with existing legislation and best practice procedure to be admissible in a trial. Although the details differ depending on national legislation, the following basic criteria must generally be taken into account.


Hessisches Ministerium der Justiz

HESSEN

# Considerations for Electronic Evidence

**Authenticity**: It must be possible to positively tie evidentiary material to the investigated incident.

**Completeness**: It must tell the whole story and not just a particular perspective.

**Reliability**: There must be nothing about how the evidence was collected and subsequently handled which causes doubt about its authenticity and veracity.



HESSEN

# Considerations for Electronic Evidence

**Believability**: It must be readily believable and understandable to a judge and/or the members of a jury.

**Proportionality**: its application to Digital Forensics establishes that the whole investigative process must be adequate and appropriate: the benefits that are to be gained by using a specific measure must outweigh the harms for the party or parties affected by the measure.

BELIEVABILITY MATTERS






HESSEN

# Expert Witness

- Technical ability
- Industry background
- Excellent teaming ability
- Excellent communication skills

HESSEN

# Presentation in Courtroom

- Establishing the link between “digital” and “human” domains (attribution):

  No fingerprints or DNA in cyberspace

- Presentation of “technology” to the jury and judge:

  Technical terms only if necessary

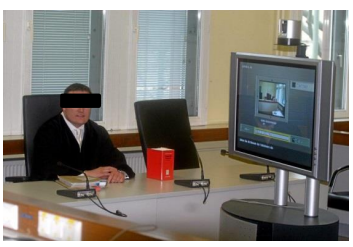
- *Make the crime real*

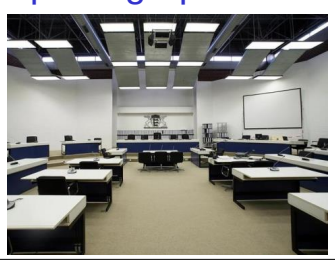
Hessisches Ministerium der Justiz

HESSEN

# Presentation in Courtroom

- Presentation of electronic evidence to the court is more effective if it is visual.
- Research has found that many people give more attention to what they see rather than hear.
- Since a prosecutor’s duty is to put forward the prosecution case in the best possible light, visual presentation of evidence especially in complicated cases is advisable.
  .
- Presentation of electronic evidence to the court is more effective if it is visual, using projector devices, PowerPoint presentations, video demonstrations, computer graphics and flipcharts.





## Presentation in Courtroom

- Get the court's permission in advance for your electronic presentation.
- Try to get a feeling for the judge's concerns about the technology and adapt accordingly.
- Don't overdo the technological presentation.
- Be sure that the technology is working, visit the courtroom site in advance of the proceedings and check!





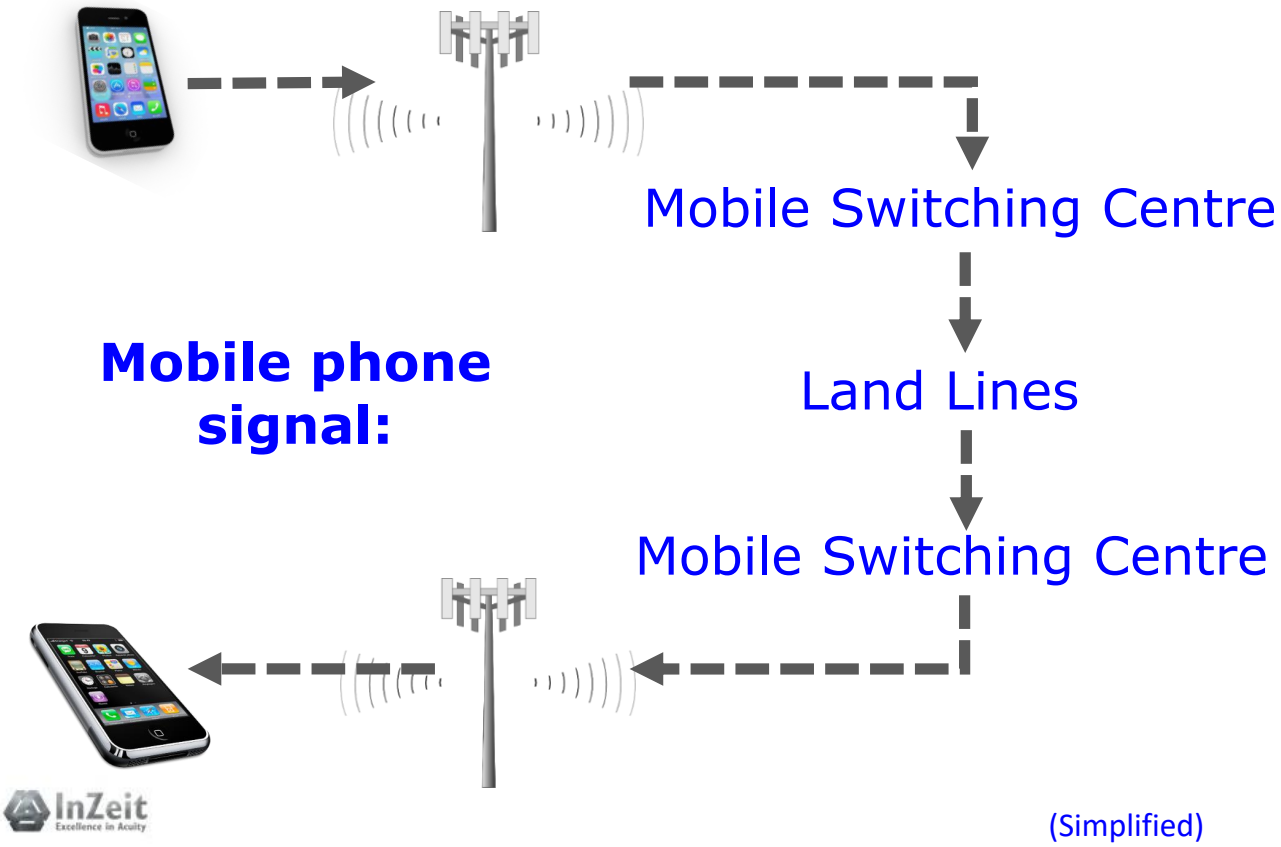

Thank you for your attention!
Questions? Remarks?


**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
Excellence in Acuity




**Mobile phone signal:**

(Simplified)

# Phones

Identifiers:

**SIM** (Subscriber Identity Module) Card

**IMEI** International Mobile Equipment Identity
– fixed to phone

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

**IMSI** International Mobile Subscriber Identity
– linked to SIM/Account

Subscriber Account details

# 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 Excellence in Acuity

# 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) 'up to' 20 Gigabits per second. Lots of small cell stations (30-300GHz) more affected by weather and obstacles.

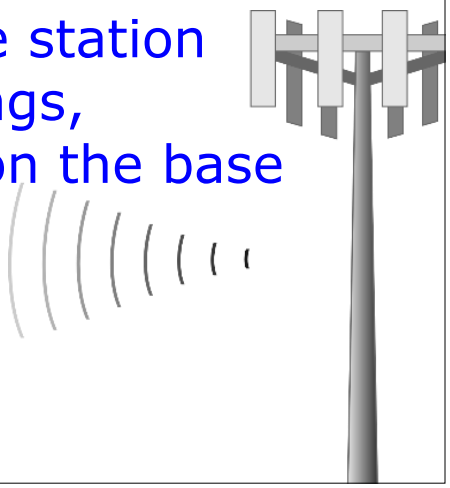
InZeit Excellence in Acuity

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
Excellence in Acuity

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.

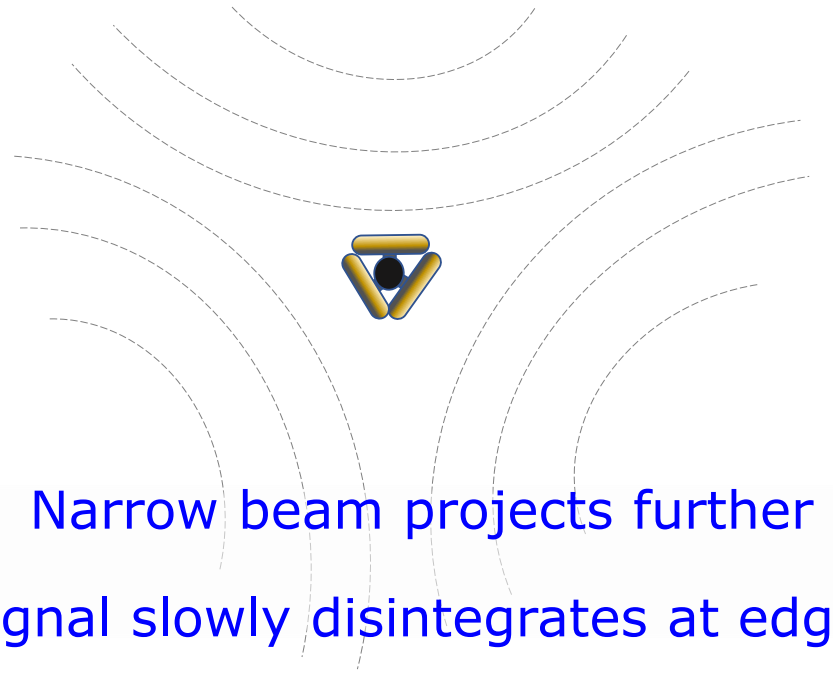

InZeit
Excellence in Acuity

## 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

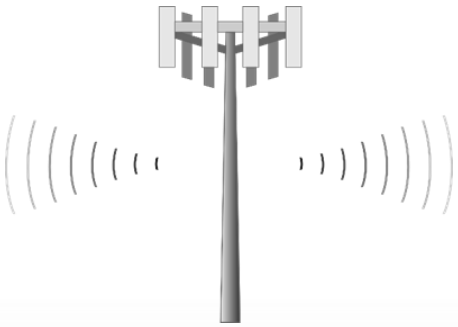
Depending on number of dishes, one dish may cover 60° - 180° (here 120° sector shown)



Narrow beam projects further

Signal slowly disintegrates at edges

InZeit Excellence in Acuity



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 Excellence in Acuity

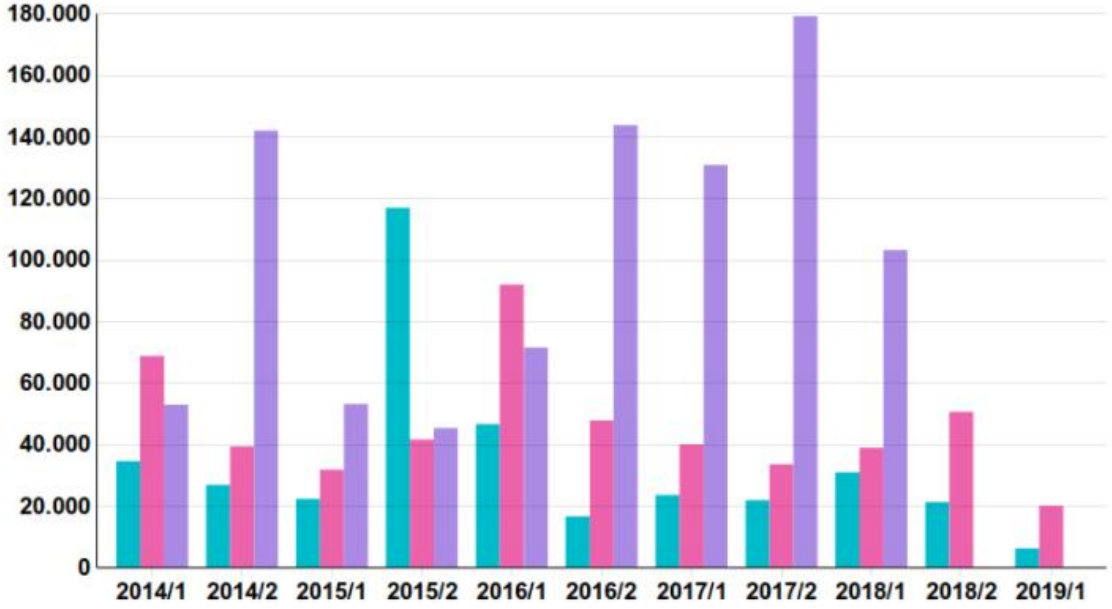
## Time difference of arrival (TDOA)


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

InZeit Excellence in Acuity

# Stealth (sms) Ping

## Causes phone to register on (nearest) mast

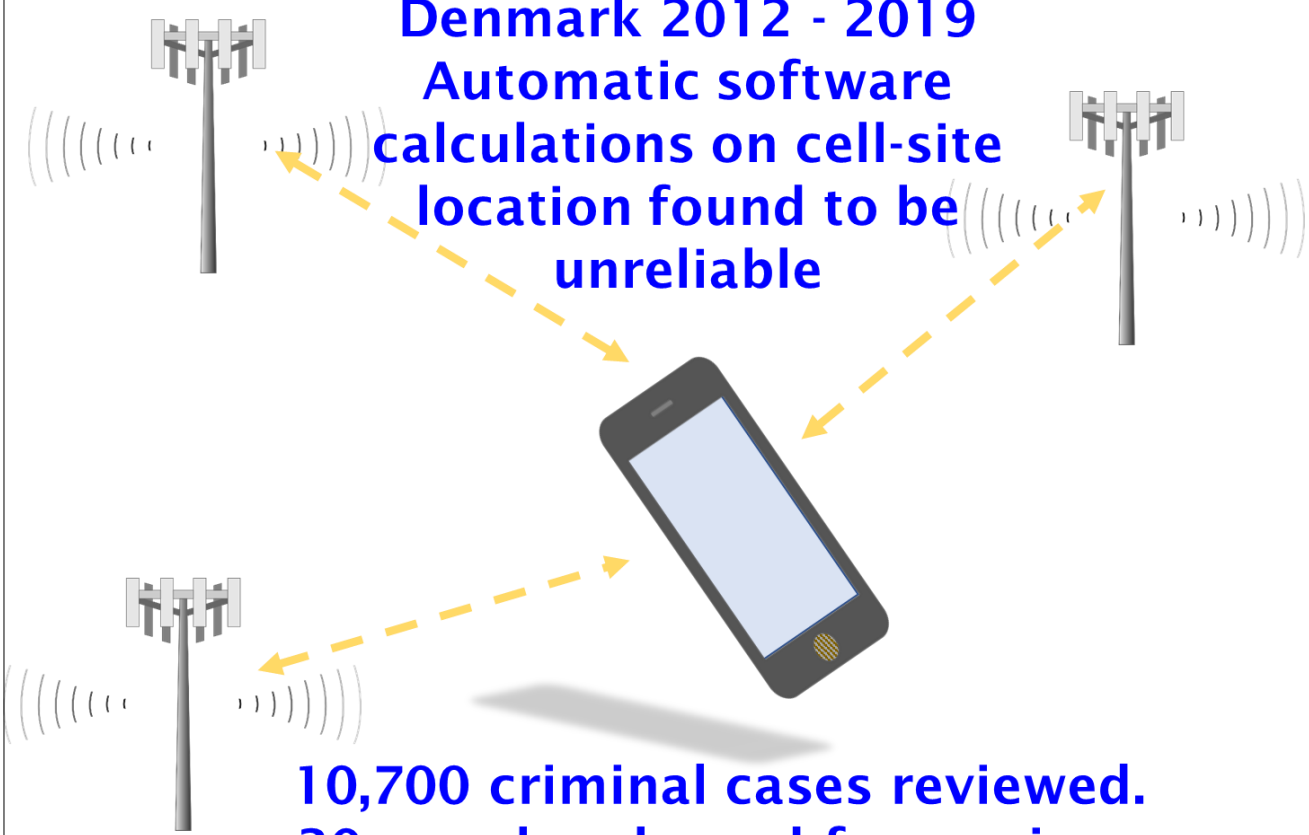



**BKA Federal Criminal Police**
**BPOL Federal Police**
**BfV Federal Office for the Protection of the Constitution**

(Commercial services: celltrack.co.uk, geocell.mobi)

InZeit Excellence in Acuity

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



# 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 Excellence in Acuity

**Oregon Offender Search**

**Public Information (Last Updated: 04/15/2014 18:48:35)**

SID# 14776586

**Offender Name:** Roberts, Lisa Marie
**Age:** 48 **DOB:** 06/1965
**Gender:** Female **Race:** Black - African American
**Height:** 5' 04" **Hair:** Black
**Weight:** 170 lbs **Eyes:** Brown
**Caseload:** 15704 Sanjines, Cecilia

**Location:** Coffee Creek Correctional Facility
**Status:** Inmate
**Institution Admission Date** 12/02/2004
**Earliest Release Date:** 09/03/2016

Offenses | Names

| Docket Number | County | Crime | Sentence Type | Begin Date | Termination Date |
|---|---|---|---|---|---|
| 020834931/01 | MULT | MANSLAUGHTER I | Inmate Sentence | 12/02/2004 | - |

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

**Oregon Offender Search**

**Public Information (Last Updated: 04/15/2014 18:48:35)**

SID# 14776586

**Offender Name:** Roberts, Lisa Marie
**Age:** 48 **DOB:** 06/1965
**Gender:** Female **Race:** Black - African American
**Height:** 5' 04" **Hair:** Black
**Weight:** 170 lbs **Eyes:** Brown
**Caseload:** 15704 Sanjines, Cecilia

**Location:** Coffee Creek Correctional Facility
**Status:** Inmate
**Institution Admission Date** 12/02/2004
**Earliest Release Date:** 09/03/2016

Offenses | Names

| Docket Number | County | Crime | Sentence Type | Begin Date | Termination Date |
|---|---|---|---|---|---|
| 020834931/01 | MULT | MANSLAUGHTER I | Inmate Sentence | 12/02/2004 | - |

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

# GPS

InZeit
Excellence in Acuity

## 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)

InZeit
Excellence in Acuity

# Geofence Warrants & Google's Sensorvault

Who has an Android phone?

72.84% Android Global Market Share

(June 2021) statista.com

Location data saved to 'Sensorvault' database

InZeit Excellence in Acuity

# Sensorvault

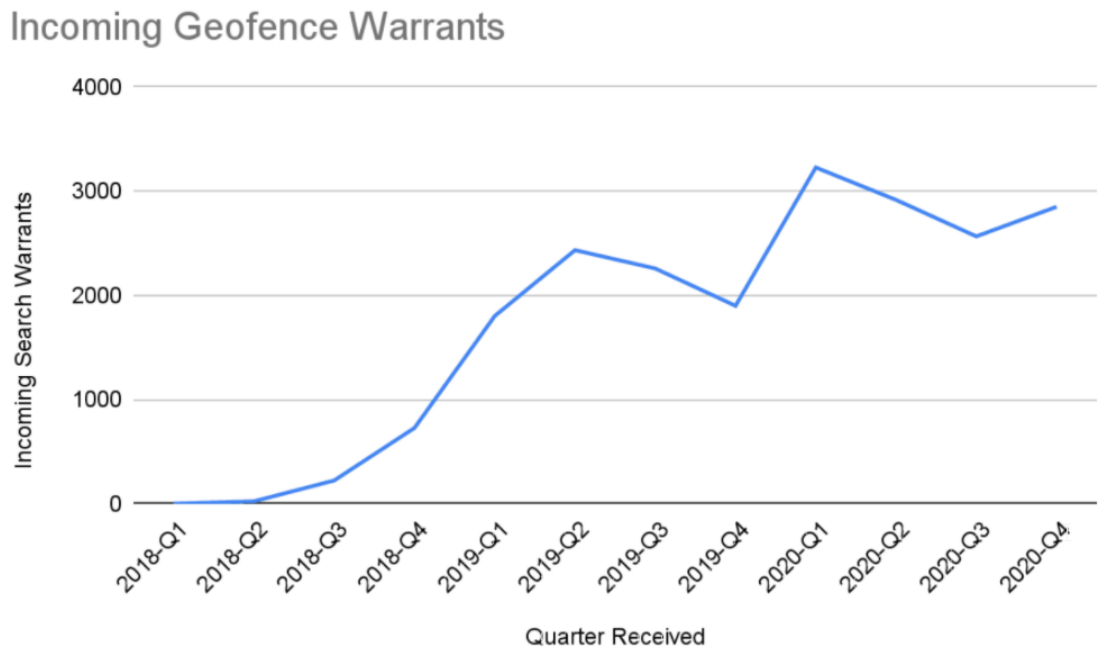
Google's Sensorvault database contains location data for hundreds of millions of devices all over the world.

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.

InZeit Excellence in Acuity




**25% of all US warrants received by Google in 2020**

InZeit Excellence in Acuity

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

Milwaukee, Wisconsin, USA June 2017

Middle of the night - Woman car jacked by 2 males

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

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

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

InZeit Excellence in Acuity

Geofence Warrant sought & obtained within 12 hours

Forwarded to Google flagged “exigent circumstances”

20 minutes later Google called back

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

InZeit Excellence in Acuity

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

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

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

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

5 Days from crime report to arrest – DIFFERENT STATES.

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


InZeit Excellence in Acuity

**Milwaukee to Louisville 400 miles (650km)**

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

InZeit Excellence in Acuity

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

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

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/

## Location Based Services

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

InZeit
Excellence in Acuity

## 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)

InZeit
Excellence in Acuity

Your location traded commercially with your ‘consent’

Thinknear suggests 54% of reported LBS locations are out by more than 1000 metres.

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

InZeit
Excellence in Acuity

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.

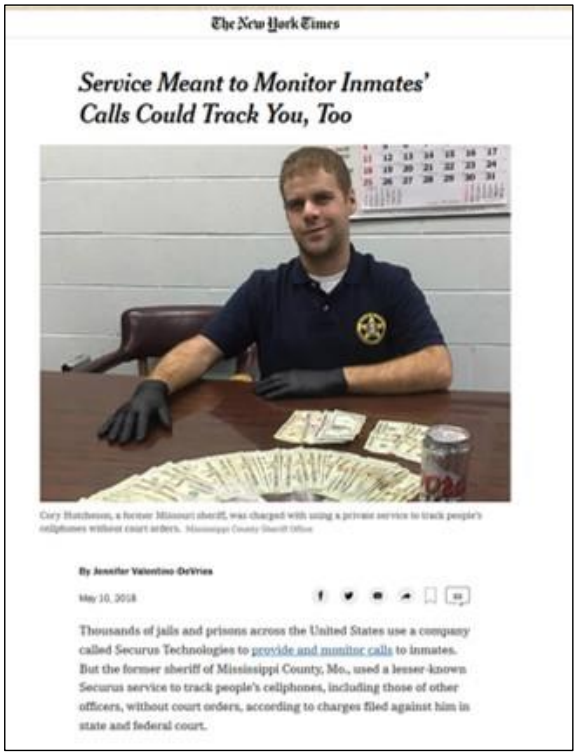
Data legitimately used for search & rescue finding lost/missing persons or fugitives.

The information is ‘volunteered’ by phone users through phone contract terms.

InZeit
Excellence in Acuity

(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*

Cory Hutcheson, a former Missouri sheriff, was charged with using a private service to track people's cellphones without court orders. Mississippi County Sheriff's Office

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

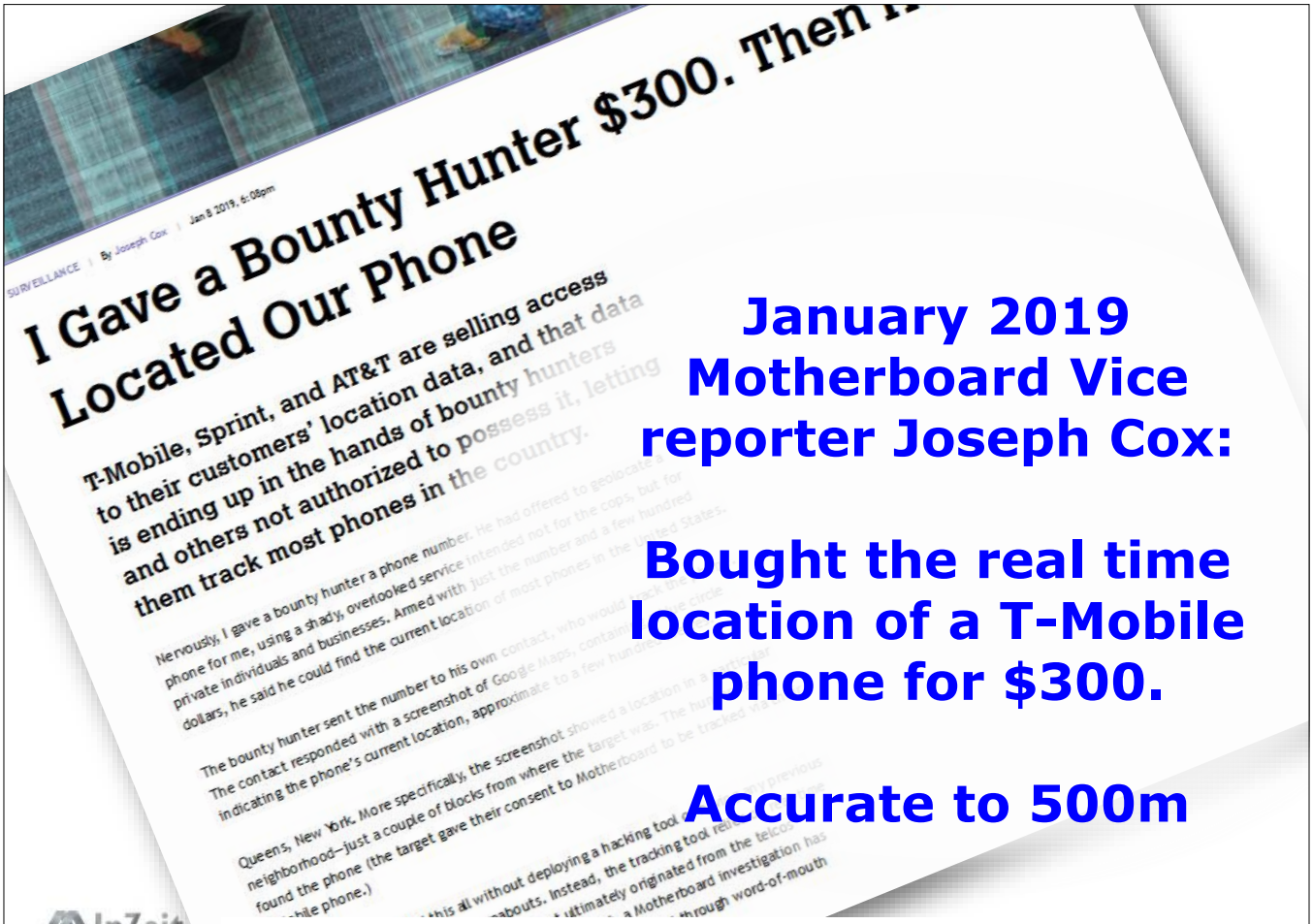
InZeit
Excellence in Acuity

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




https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

COURTHOUSE NEWS SERVICE

# Class Claims AT&T Sold Their Real-Time Locations to Bounty Hunters

*Despite assurances to the contrary, AT&T has been selling its customers' location data to creditors, bounty hunters, landlords, prison officials, and all sorts of third parties, according to data privacy watchdog Electronic Frontier Foundation in a federal class action filed Tuesday.*

MARIA DINZEO / July 16, 2019

https://www.courthousenews.com/class-claims-att-sold-their-real-time-locations-to-bounty-hunters/

ELECTRONIC FRONTIER FOUNDATION

About Issues Our Work Take Action Tools Donate

**Scott v. AT&T - Order Dismissing Case** 16.02.2021

NORTHERN DISTRICT OF CALIFORNIA

KATHERINE SCOTT, et al.,
Plaintiffs,
v.
AT&T INC., et al.,
Defendants.

Case No. 19-cv-04063-SK

**ORDER REGARDING MOTION TO DISMISS AND MOTION TO COMPEL ARBITRATION**

Regarding Docket Nos. 35, 73, 106, 117, 132, 141

https://www.eff.org/document/scott-v-att-order-dismissing-case

**Telecoms companies**

**Location Aggregators**

- **Zumigo**
- **Locationsmart**
- **Microbilt**

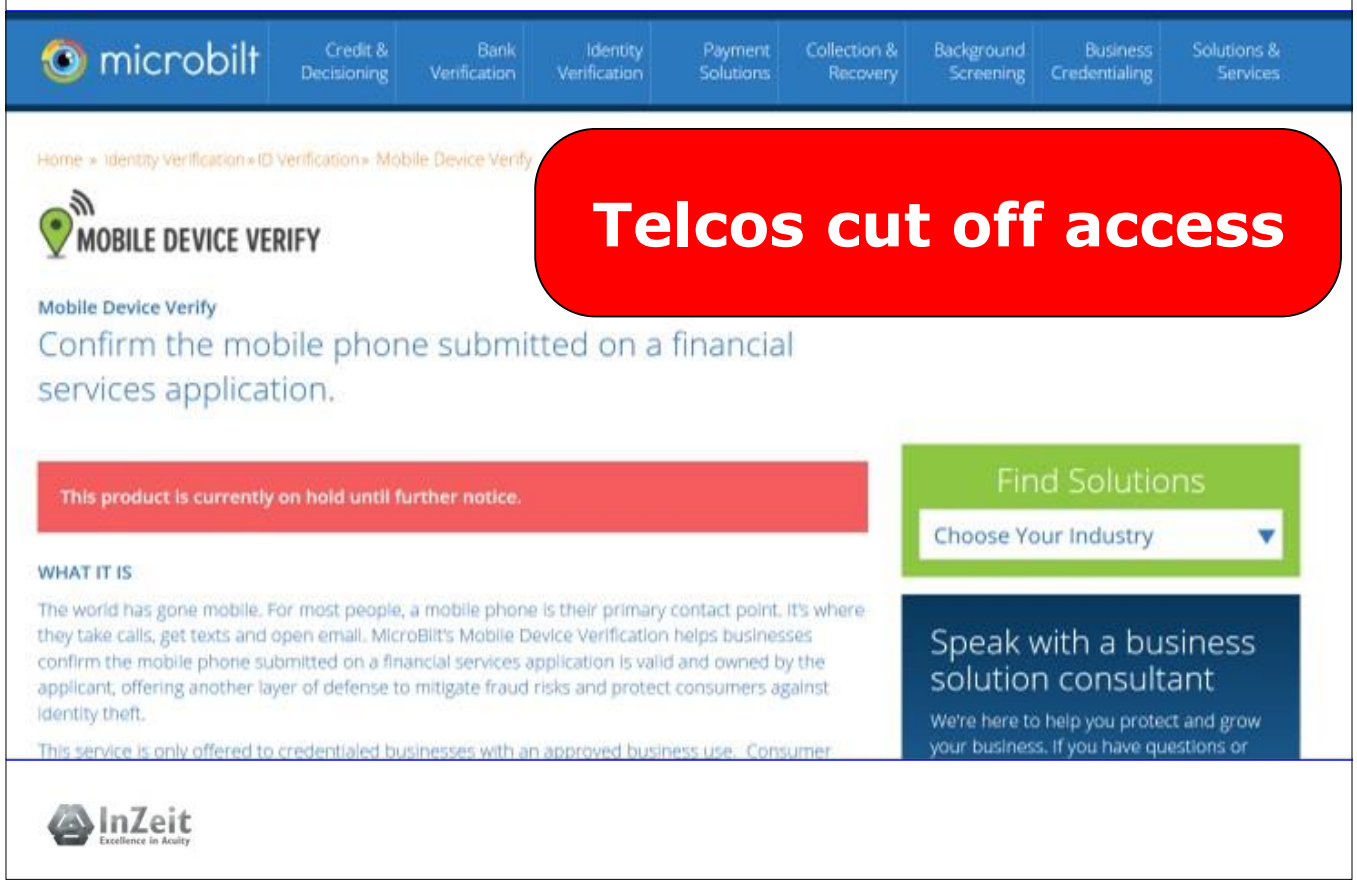
**End user clients**

**Mobile Device Verify tool**

**Bounty Hunters**
**Debt Collectors**
**Background checks on tenants**
**Roadside assistance**
**Bank fraud**

# Black market

InZeit
Excellence in Acuity




InZeit
Excellence in Acuity

# IMSI Catcher
## (aka StingRay, Hailstorm, TriggerFish)

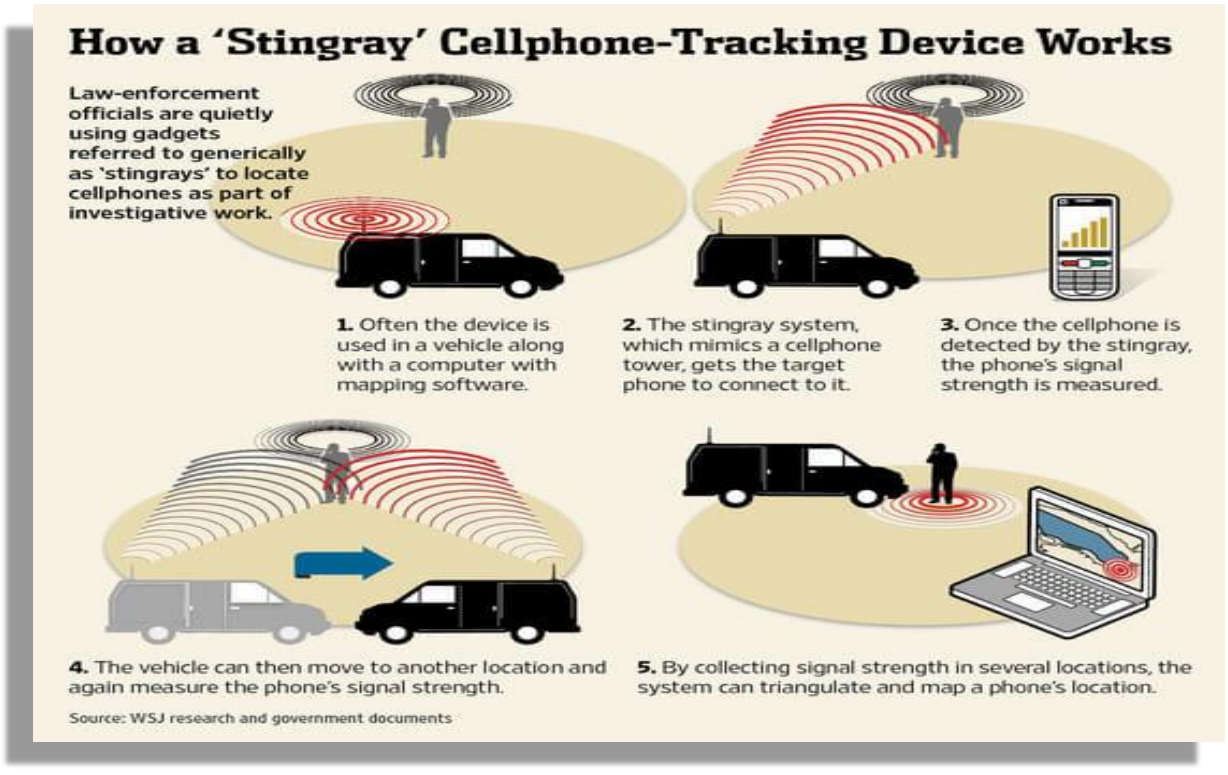
Device imitates mobile phone base station

Phone automatically detects & connects to the IMSI catcher

All phone traffic passes through the IMSI catcher

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

InZeit
Excellence in Acuity




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

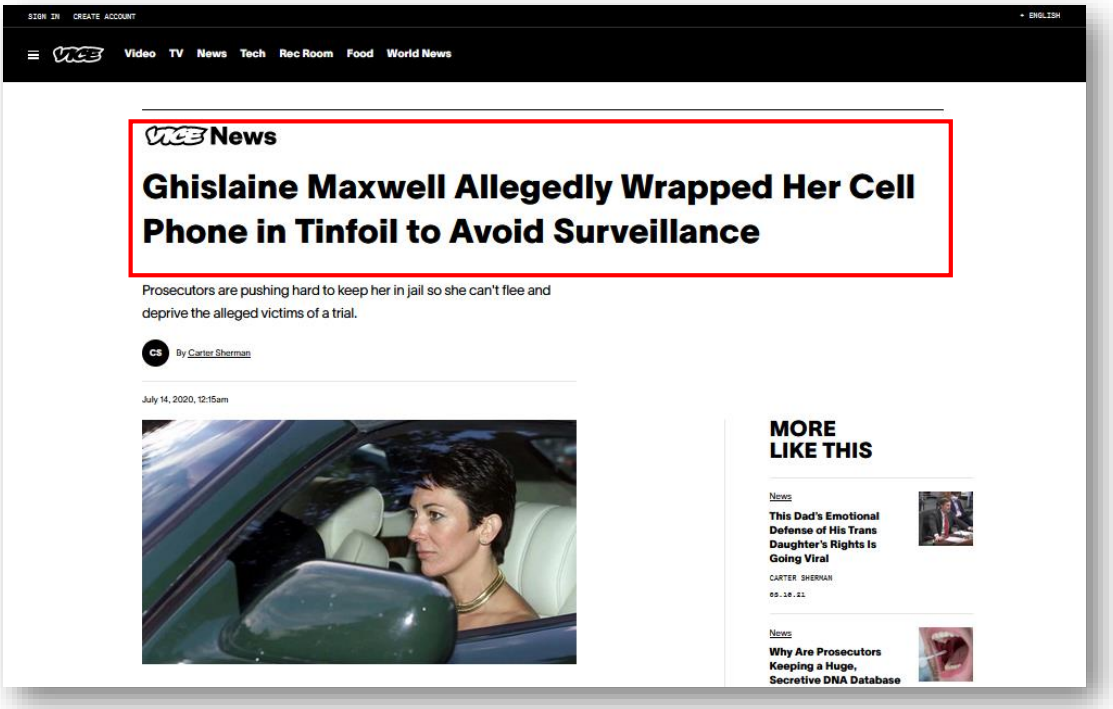
InZeit
Excellence in Acuity

# 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

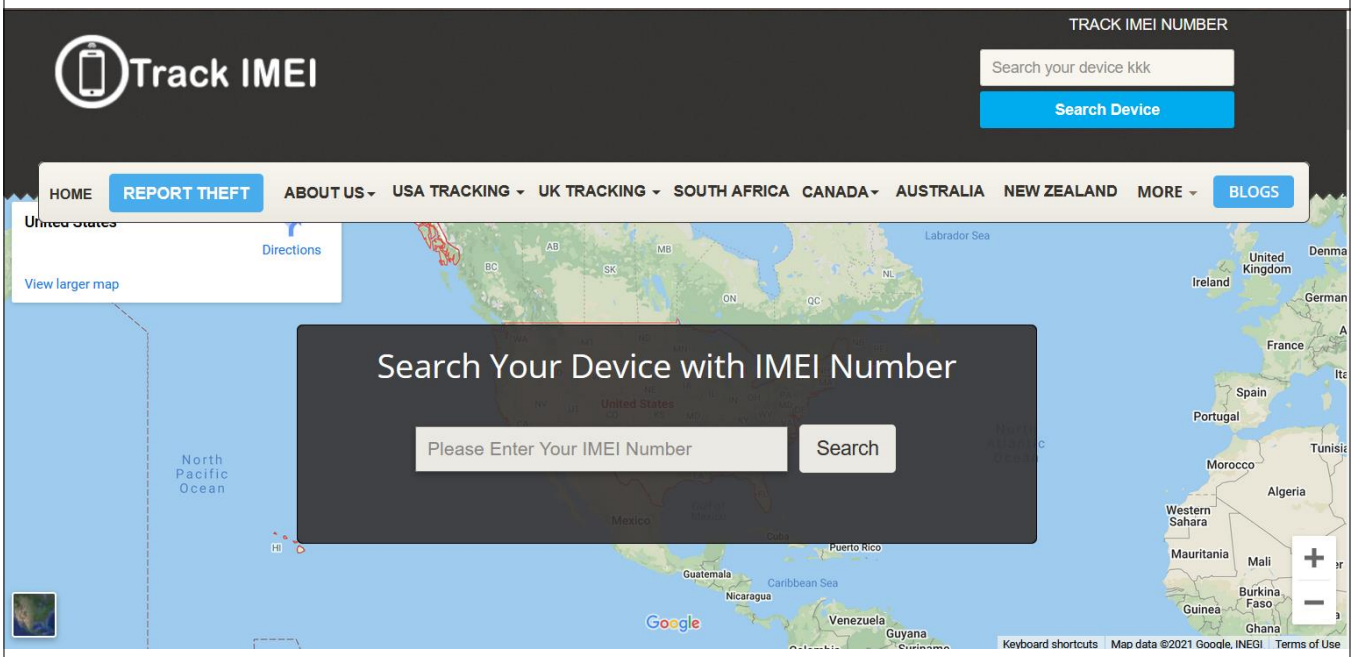
InZeit
Excellence in Acuity

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

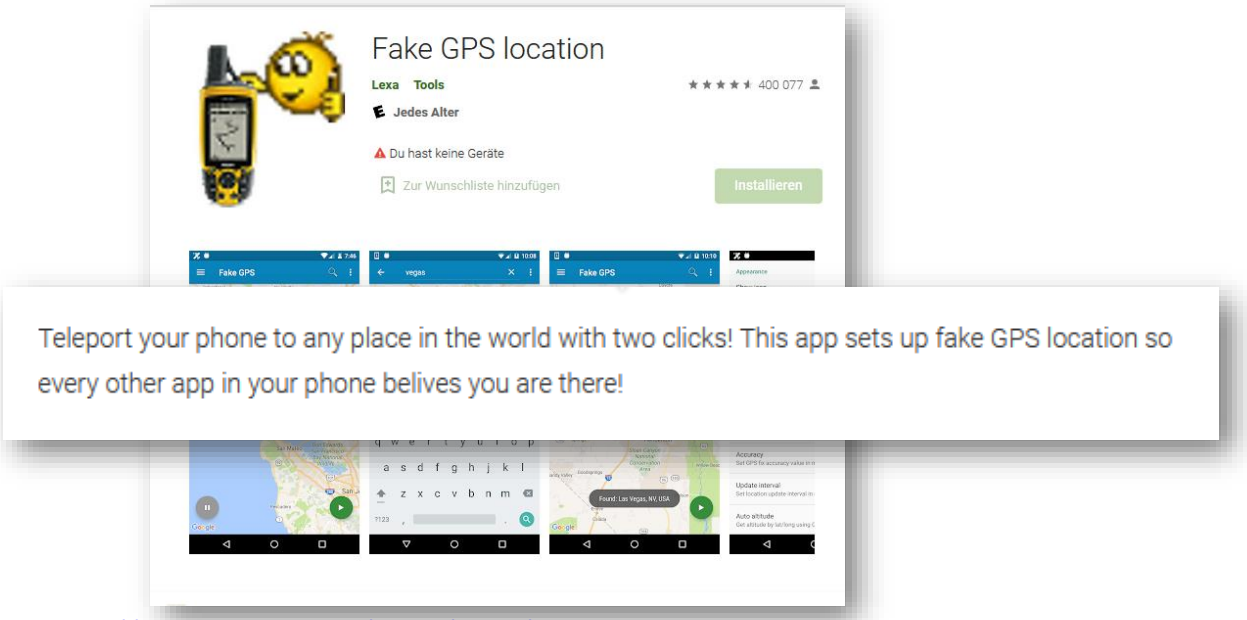



## 'Cell phone data' (GPS and/or cell site analysis) > 1 square mile (2.59 km$^2$)

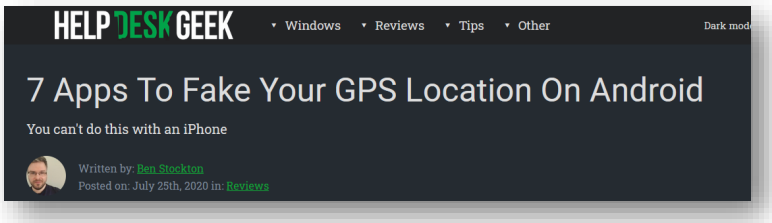
InZeit
Excellence in Acuity




https://trackimei.net/




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/

# Summary

**Phone location evidence not as accurate as often portrayed**

**Influenced by lots of factors (technical/topographical/meteorological)**

**Nevertheless powerful tool**

**Can be used to establish historical movements**

**Tendency to trust technology blindly**

**Our personal data is traded for profit**

InZeit
Excellence in Acuity

info(at)inzeit(dot)eu

InZeit
Excellence in Acuity

# *Some Reference Material*

InZeit
Excellence in Acuity


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

Dinzeo,M.(2019) *Class Claims AT&T Sold Their Real-Time Locations to Bounty Hunters* https://www.courthousenews.com/class-claims-att-sold-their-real-time-locations-to-bounty-hunters/

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 https://www.gps.gov/systems/gps/performance/accuracy/

Hollister, S. (2019) 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



InZeit
Excellence in Acuity

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/

Mackey, A. (2021) *Forced Arbitration Thwarts Legal Challenge to AT&T's Disclosure of Customer Location Data* https://www.eff.org/deeplinks/2021/04/forced-arbitration-thwarts-legal-challenge-atts-disclosure-customer-location-data

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

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

Scott v AT&T Court Order https://www.eff.org/document/scott-v-att-order-dismissing-case



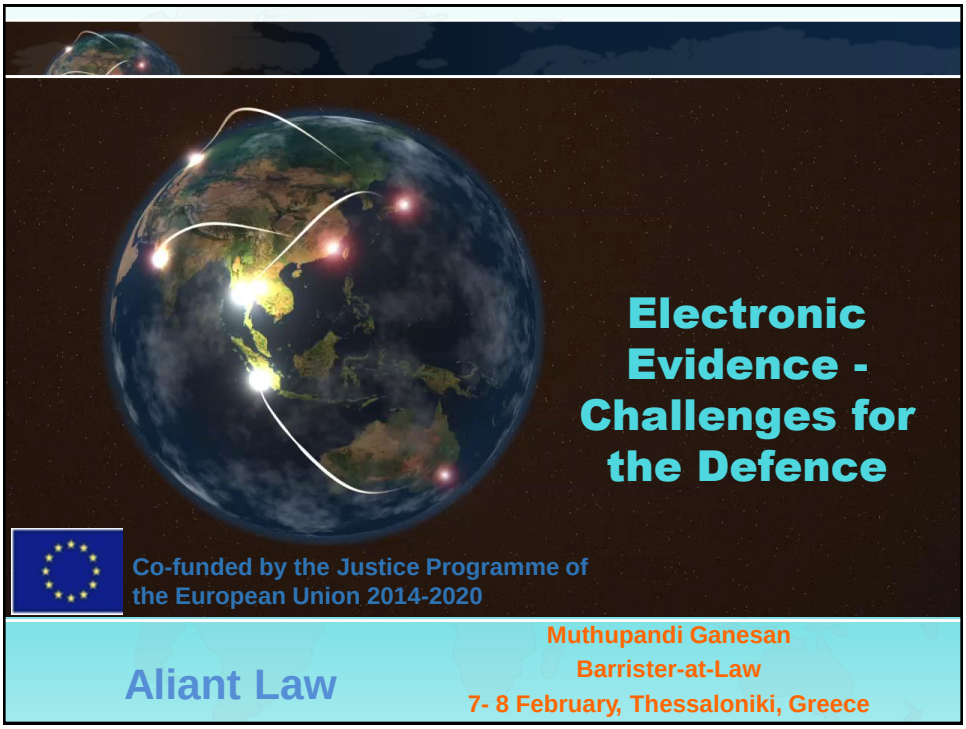
U of Derby DECM (2019) *Accuracy of Location Services on Smart Devices* Blog https://computing.derby.ac.uk/c/accuracy-of-location-services-on-smart-devices/

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

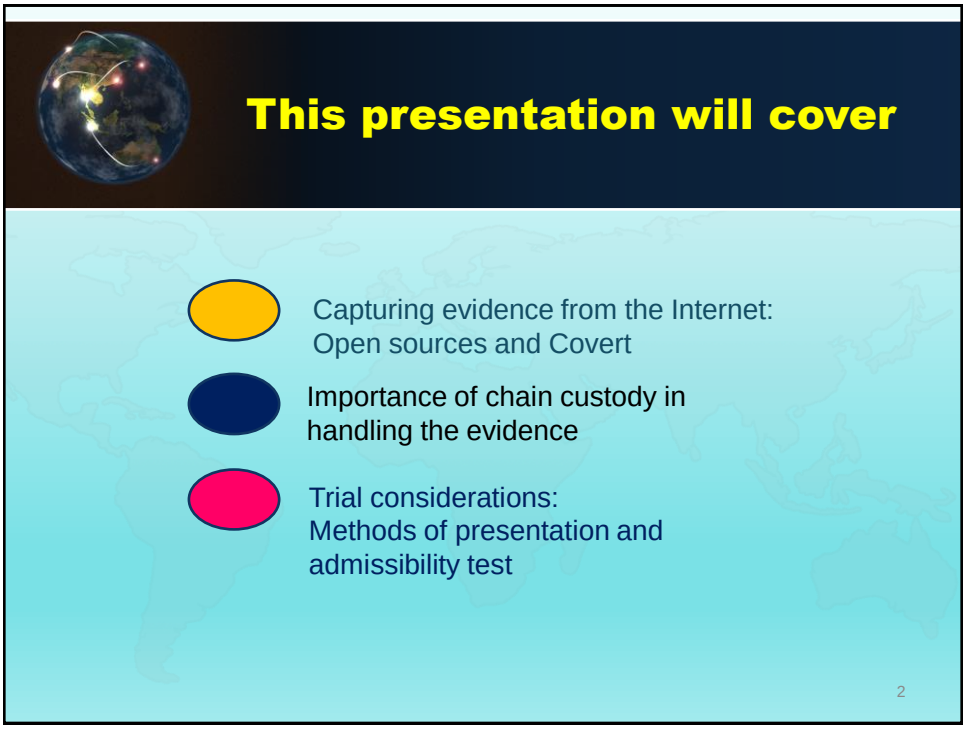
Valentino-DeVries, J. (2018) Service Meant to Monitor Inmates' Calls Could Track You, Too New York Times (10/05/2018)

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/

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


Electronic Evidence - Challenges for the Defence
Co-funded by the Justice Programme of the European Union 2014-2020
Aliant Law
Muthupandi Ganesan
Barrister-at-Law
7- 8 February, Thessaloniki, Greece

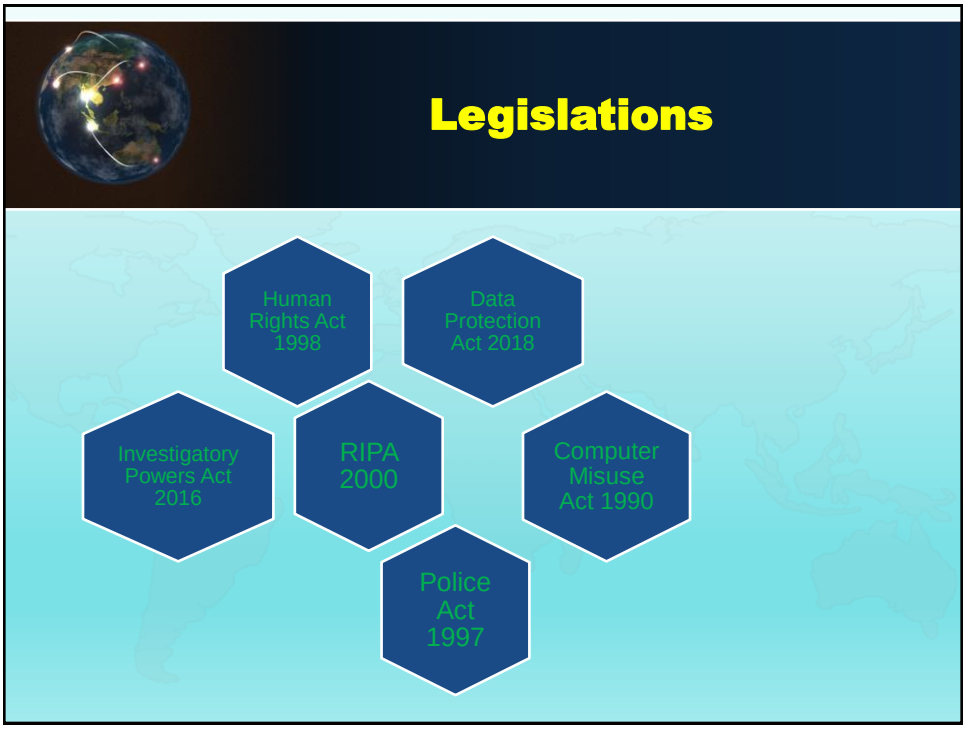
1


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

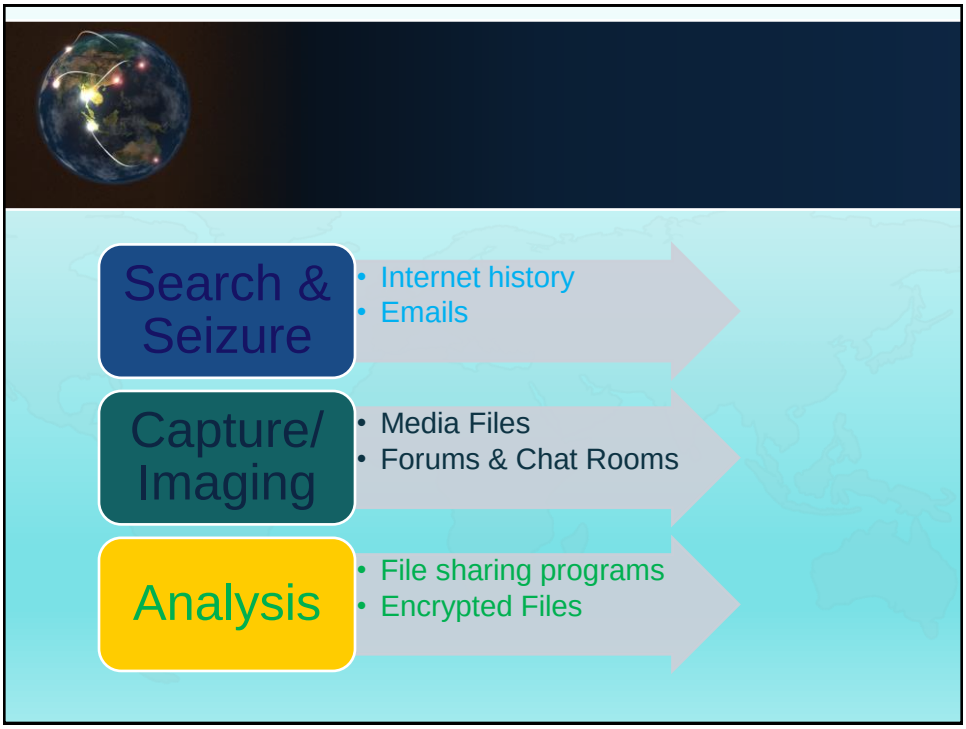
2


Open Source
Echosec
Social Media
Geofeedia
Financial Sites
Social Searcher
Publications

3


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

4


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

5


Witness Statements
Reports
Expert Evidence

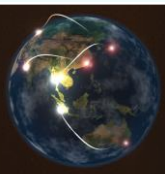
6

NPCC Guidance on Open Source Investigation / Research

ACPO – Good Practice Guide for Digital Evidence – March 2012

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

7



# General principles

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

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

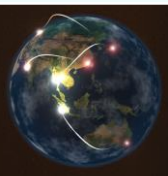
**(ii) In circumstances where a person finds it necessary to access original data held on computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and implications of their actions;**

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

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

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

8

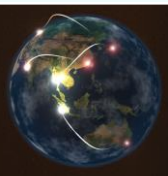


# Digital evidence – International Issues

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

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

9



# Types of guidance

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

10

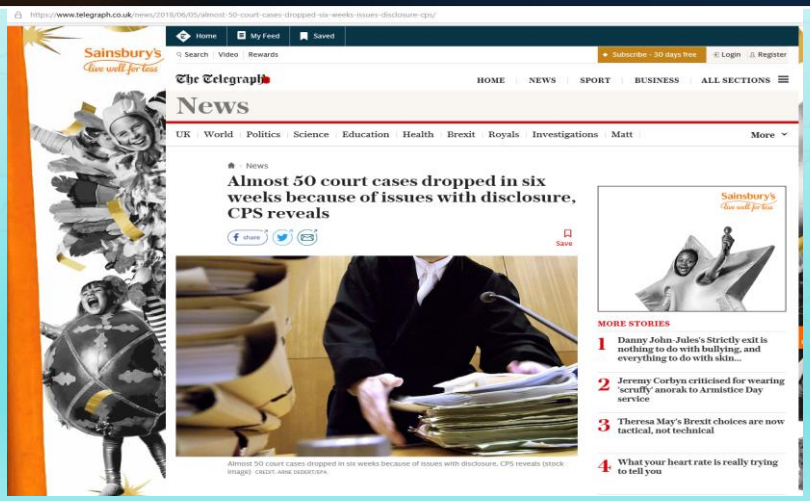
# Disclosure – Practical Issues

- Volume of Data
- Funding
- Equipment
- TRAINING:

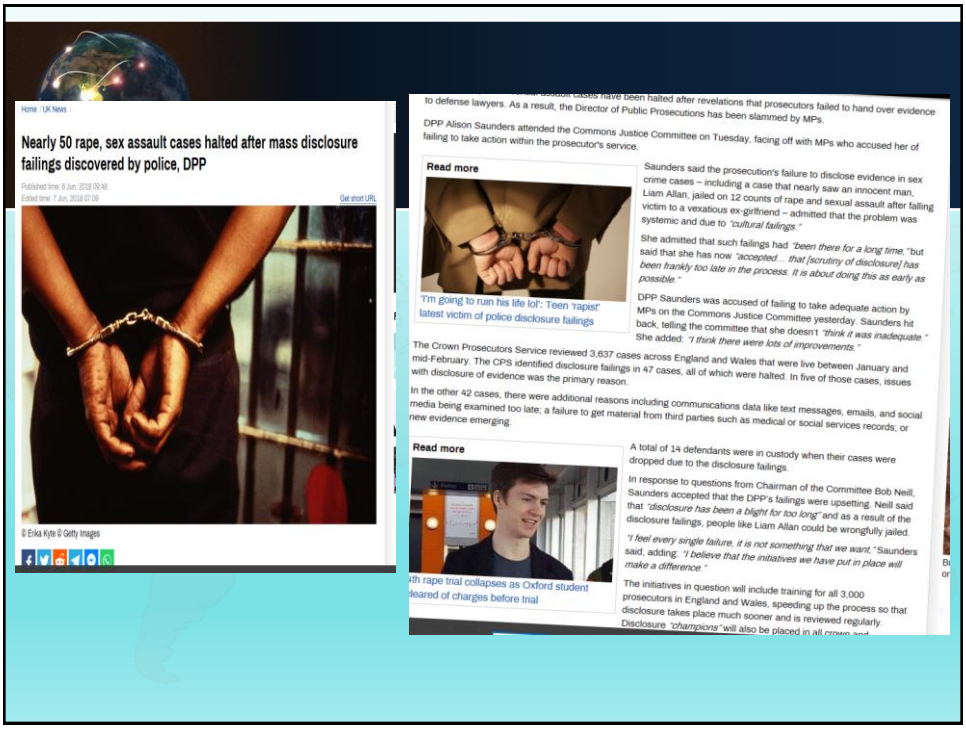
  For Judges, Prosecutors, Defence Lawyers and Clients
- NATURE OF EVIDNECES:

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

11




12

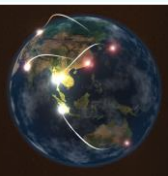



13

# DISCLOSURE: QUALITY OF KNOWLEDGE : JUDGE VERSUS JURY

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

14

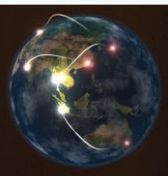


# EXPERT EVIDENCE IN DIGITAL / CLOUD COMPUTING

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

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

15



# Expert Witness

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

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

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

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

16

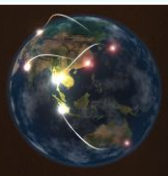
# Expert evidence: Challenges

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

17

# Expert evidence: expertise must be reviewed carefully!


18



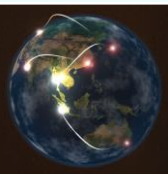
# Cybercrime Legislation

**Functions of cybercrime legislation**

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



19



# Cyber crime legislation

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



20

# Cyber crime legislation: Problems

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

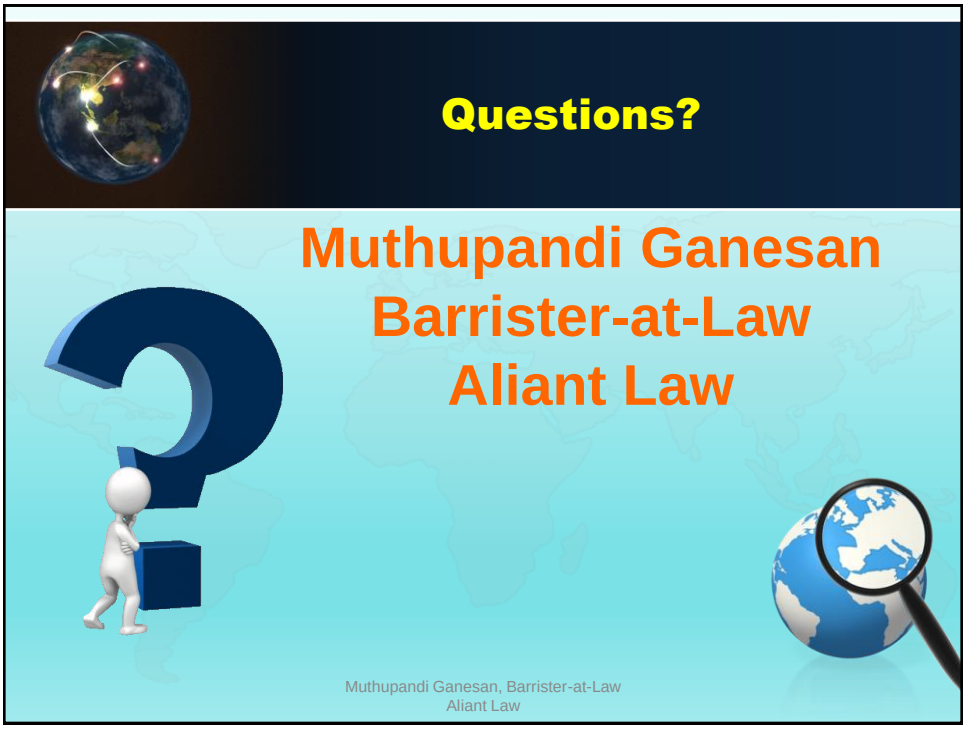
21

# Complexity


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



22


Questions?
Muthupandi Ganesan
Barrister-at-Law
Aliant Law
Muthupandi Ganesan, Barrister-at-Law
Aliant Law

23

# 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

Deputy prosecutor

Public Prosecutor´s Office to the Athens Court of First Instance

LLM IT Law (London)

LLM Penal Sciences (Athens)

Thessaloniki, 07-08 Febrruary 2022

1

# Why e-evidence is so important?

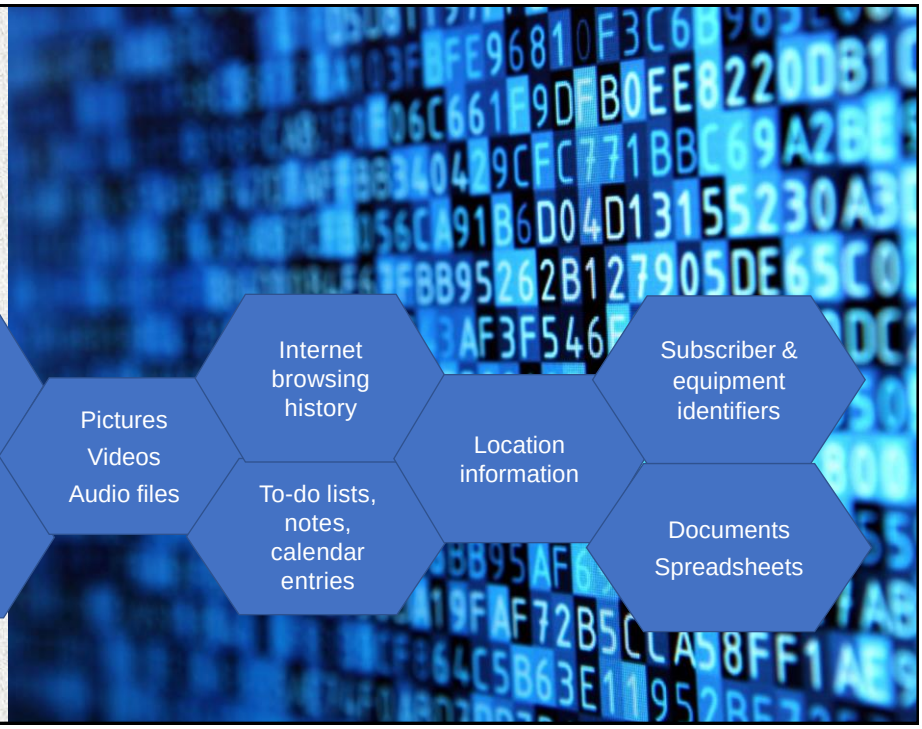
More and more crimes committed online and facilitated by electronic devices such as mobile devices ➡ traces of the crimes are left on these devices.

HOWEVER, e- evidence is

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

2

## Digital evidence on a mobile device (a non - exhaustive list)




3

## Digital 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)

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 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.

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

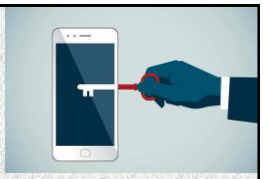
- Be present during the research and seizure of digital data
- Appoint a technical consultant who has the right to be present during the examination of the evidence, comment on the findings of the report of the Digital Forensic Department and draft a report with his / her proper findings (art.204,207,208 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.

### 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.

9

## What happens if you can't unlock the mobile?


erhui1979 / Getty Images

- 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)

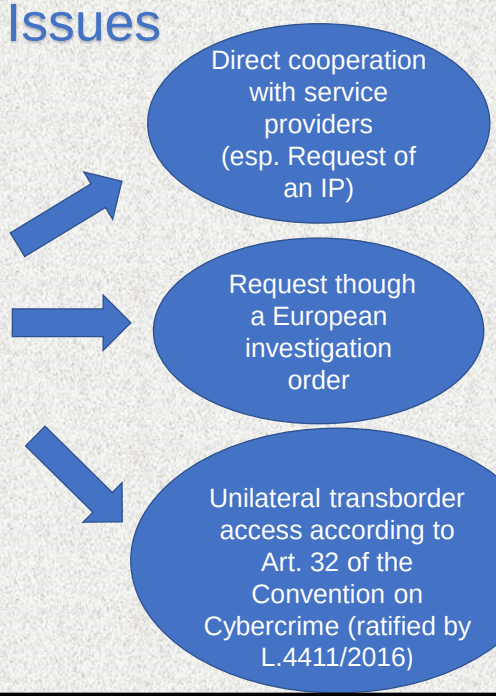
⬇

Possible criminal liability for harboring the offender ?

10

# Jurisdictional Issues

**Search and seizure of extraterritorially located data**




11

# 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 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.

12

## 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)

13

## 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.

Tha accounts were seized and hard disks, laptops, mobile phones, SIM cards and micro sd cards were also 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

14

## 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....

15

## 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 taκen 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.

16

# Thank you

Questions?

17