30 YEARS ERA

# OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

FOCUS ON THE WHOLE LIFE CYCLE OF E-EVIDENCE (CUSTODY CHAIN, PRESENTATION & ASSESSMENT)

Cracow, 24-25 March 2022

UP GRADE YOUR LEGAL EXPERTISE

Criminal Law

## Speakers

**Linda Bertram**, Public Prosecutor, Cybercrime Centre, Prosecutor General's Office, Frankfurt am Main

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

**Maša Galič,** Assistant Professor, Privacy and Procedural Criminal Law, Criminal Law and Criminology Department, Vrije Universiteit (VU), Amsterdam

**Anna Illamaa,** Police- and Border Guard Board, North Prefecture; Serious Crime Unit, Digital evidence group Special investigator, Tallinn

**Tomasz Iwanowski,** Public Prosecutor, Head of Cybercrime Division at National Prosecutor's Office, Warszawa

**Damir Kahvedžić,** Solutions Advisor and Operations Manager, ProSearch, Dublin

**Agnieszka Kluczyńska-Cichocka,** Head of International Cooperation Department, National School of Judiciary and Public Prosecution. Lublin

**Emmanuelle Legrand,** Magistrate, AI Project Manager, Digital Economy Department, Ministry of the Economy, Finances and Recovery, Paris

**Bilal Sen,** Senior Investigator, Coninsec, Cologne

**David Silva Ramalho**, Defence Lawyer, Morais Leitão, Galvão Teles, Soares da Silva & Associados; Lecturer, Faculty of Law, University of Lisbon

**Branko Stamenkovic,** Prosecutor, High-Tech Crime, Belgrade; Member of the European Judicial Cybercrime Network (EJCN), The Hague

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

## Key topics

- The foundations of electronic evidence (direct and indirect evidence, primary and secondary evidence, ownership of digital data)
- Collecting, authenticating and evaluating digital data in the framework of legal proceedings
- The challenges posed by encrypted data
- Search orders, search and seizure, destruction of evidence, evidence from other jurisdictions, trial
- Chain of custody (through case studies)

Language
English

Event number
322DT03f

Organisers
ERA (Laviero Buono) in cooperation with the Polish National School of Judiciary and Public Prosecution

KRAJOWA SZKOŁA SĄDOWNICTWA I PROKURATURY

european.law

# OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

## Thursday, 24 March 2022

08:30 Arrival and registration of participants

09:00 **Welcome and introduction to the programme**
*Agnieszka Kluczyńska-Cichocka & Laviero Buono*

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

*Chair: Laviero Buono*

09:15 **Internet searches and computer forensics: using open source intelligence to gather evidence online**

- Internet 1.0/2.0 vs social media 1.0/2.0
- Internet cache: deleting & retrieving
- Hidden features of websites to help you gather unseen evidence: real life examples from select websites and social media
- Best practices on how to gathering online evidence correctly and avoid common pitfalls
- Analysis techniques to investigate evidence effectively
- Demonstration of evidence gathering tools

*Damir Kahvedžić*

10:00 Discussion

10:15 **Examination of digital devices, such as computers, mobile phones, media storage (USB, memory cards, etc.)**

- File systems (NTFS, macOS, Linux)
- Windows and MacOS artefacts
- Chain on custody & digital evidences handling

*Anna Illamaa*

11:00 Discussion

11:15 Break

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

*Chair: Damir Kahvedžić*

11:45 **Covert internet investigations online and legal hacking by law enforcement**

- Anti-forensics and the need for covert investigations
- Online undercover investigations: specificities and risks
- The use of malware and legal hacking to collect evidence

*David Silva Ramalho*

12:30 Discussion

12:45 Lunch break

13:45 **Open source intelligence (OSINT) tools**

- Introduction and the role of OSINT
- Understanding and searching online data
- Overview of the primary data collection sources
- An OSINT case presentation

*Bilal Sen*

14:45 Discussion

15:00 Break

*Chair: Laviero Buono*

## Objective

As a result of online investigations, almost all criminal courts are confronted with the question of whether or not electronic evidence presented in criminal proceedings is admissible. Rules governing the admissibility of electronic evidence vary in the legal framework of different Member States and are continuously challenged by the evolution of technological devices such as computers, mobile phones and digital cameras.

This seminar aims at promoting advanced knowledge, exchange of experience and best practices between judges, prosecutors and lawyers in private practice from EU Member States who are dealing with online investigations. This will improve participants' knowledge of the strategies and techniques used in different European countries and will ultimately improve cross-border cooperation among Member States' authorities.

## About the Project

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

## Who should attend?

Judges, prosecutors and lawyers in private practice from EU Member States (Denmark does not participate in the Justice Programme 2014-2020).

## Venue

National School of Judiciary and Public Prosecution
ul. Przy Rondzie 5
31-547 Cracow
Poland

## CPD

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

15:30 **Online investigations and the challenges of dealing with electronic evidence in criminal proceedings**

- Principles of dealing with electronic evidence
- Common procedures for handling evidence on digital devices
- International investigations (search and seizure – obtaining evidence from the Internet, admissibility)

*Linda Bertram*

16:15 Discussion

16:30 End of the first day and dinner offered by the organisers (19:30)

## Friday, 25 March 2022

*Chair: Bilal Sen*

09:30 **E-evidence in digital investigations with particular reference to jurisdictional issues and data production orders**

- Cross-border access to data and jurisdictional issues
- Cloud computing
- European production orders
- Shortcomings and remedies

*Maša Galič*

10:15 Discussion

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

*Chair: David Silva Ramalho*

10:30 **Special investigation techniques: a new evidentiary frontier for the judge**

- Providing the authenticity of data resulting from dark web investigations
- Challenges posed by websites and social networks
- Ensuring that data has not been altered
- Presentation of evidence in court, case studies

*Emmanuelle Legrand*

11:00 Discussion

11:15 Break

11:45 **Trial considerations: methods of presentation and admissibility tests**

- The importance of the chain of custody in handling evidence
- Best practices

*Branko Stamenkovic*

12:30 **Collecting, authenticating and evaluating digital data in the framework of legal proceedings: best practices**

- Issuing order
- Presentation in court
- Admissibility of e-evidence

*Tomasz Iwanowski*

13:00 Discussion

13:15 End of seminar and light lunch

## Your contact persons

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

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

## Save the date

**Annual Conference on Countering Terrorism in the EU 2021**
Trier, 1-3 December 2021

**Criminal Law and Human Rights: Recent ECtHR Case Law**
Online, 9-10 Dezember 2021

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

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

**Visit our website to apply online:**
www.era.int/?131066&en

# Application

**Obtaining e-evidence when investigating and prosecuting crimes**

Cracow, 24-25 March 2022 / Event number: 322DT03f/SBa

## Terms and conditions of participation

### Selection

1. Participation is only open to judges, prosecutors and lawyers in private practice from eligible EU Member States.
2. The number of places available is limited (30 places). Participation will be subject to a selection procedure.
3. Applications should be submitted before **25 February 2022.**
4. A response will be sent to every applicant after this deadline. **We advise you not to book any travel or hotel before you receive our confirmation**.

### Registration Fee

5. €225 including documentation, lunches and dinner.

### Travel expenses

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

### Accommodation

7. Two nights' hotel accommodation (23-25 March 2022) are reserved at the Polish National School of Judges and Public Prosecution in Cracow.

### Other services

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

### Participation

9. Participation at the whole conference is required and your presence will be recorded.
10. A list of participants including each participant's address will be made available to all participants unless the ERA receives written objection from the participant no later than one week prior to the beginning of the event.
11. The participant's address and other relevant information will be stored in ERA's database in order to provide information about future ERA events, publications and/or other developments in the participant's area of interest unless the participant indicates that he or she does not wish ERA to do so. A certificate of attendance will be distributed at the end of the conference.

**Apply online for**
"Obtaining e-evidence when investigating and prosecuting crimes":
www.era.int/?131066&en

### Language

English

### Contact Person

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

### Venue:

National School of Judiciary and Public Prosecution
ul. Przy Rondzie 5
31-547 Cracow
Poland

PROSEARCH

# Internet searches and computer forensics

Using open-source intelligence to gather evidence online

Damir Kahvedžić, PhD.

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

1

## Scope

### What are we talking about here?

How does the Internet work?

Internet vs social media 1.0/2.0

Hidden evidence of websites

Best practices on how to gathering online evidence correctly and avoid common pitfalls

Real life examples from select websites and social media

### What we won’t talk about

Anything too technical

Legal stuff. I am not a lawyer

We don’t have all the answers

Analysis…

PROSEARCH

CONFIDENTIAL

2

# Case Study: Elon Musk vs SEC

### The set up

Elon Musk is an active Twitter user and currently has 77M followers

He sends a Tweet on **7th Aug 2018** saying the funding is secured to take Tesla private, which does not happen.

It has 14K Retweets, 84K likes

SEC does not like this and accuses him of misleading investors.

Elon agrees for a company lawyer to pre-approve tweets about Tesla's financial health, sales, or delivery numbers — estimated or otherwise — as well as other specific subjects

### The event

Elon Musk continues to tweet

On **6th November 2021** Elon creates a Poll asking whether he should sell 10% of his stake in Tesla.

Twitter user vote in favour

Tesla shares slump

Kimbal Musk, Elon's brother, sits on Tesla's board of directors.

He sells **$108 million** of Tesla shares the day before the poll comes out and the share values drop.

### The Aftermath

SEC does not like this.

Did Kimbal know about the vote before hand?

Is this market manipulation.

How do we preserve the Twitter evidence?

How do we preserve any other social media information out there?

PROSEARCH

CONFIDENTIAL

# Case Study by the Numbers

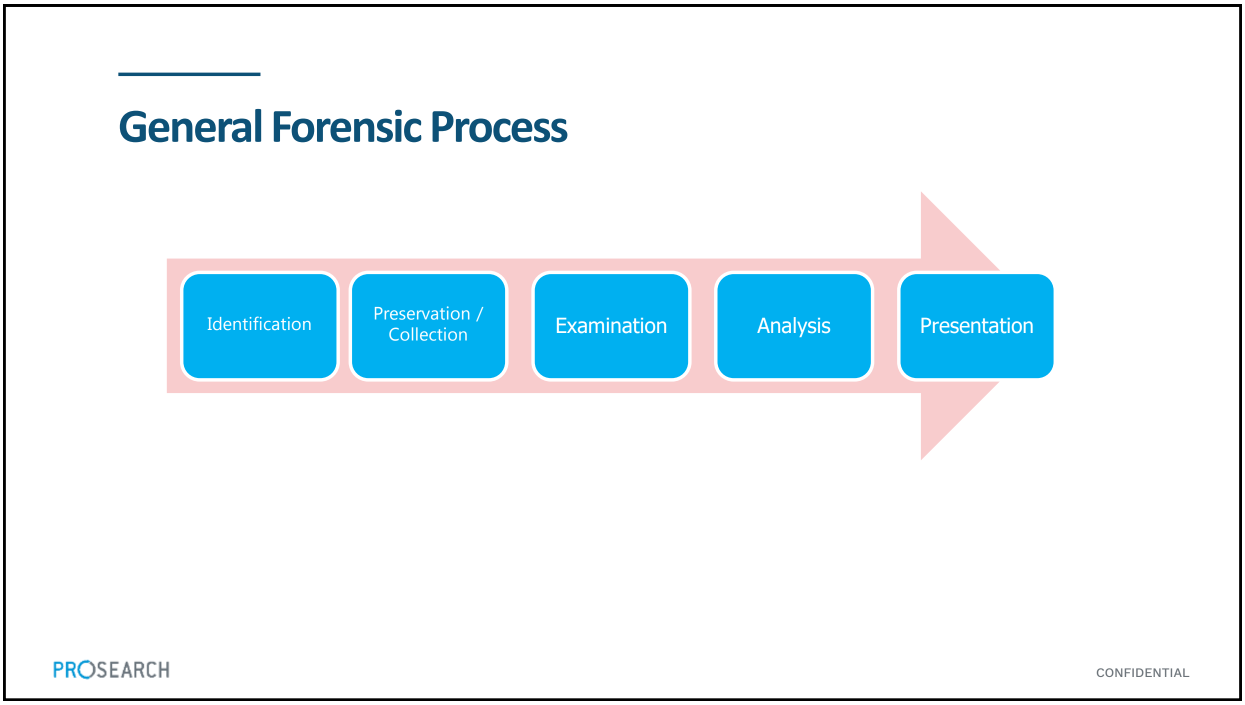
## What evidence are we looking at:

- Between 7th August 2018 and 21st November 2021 Musk Tweeted 10.5K times
- Interactions and retweets are equally important to get context
- How can we collect the Tweets and any other website information out there?

| User | Twitter Feeds | Facebook | Musk Tweets |
|---|---|---|---|
| 2 | 2 | 1 | 10.5K |

PROSEARCH

CONFIDENTIAL

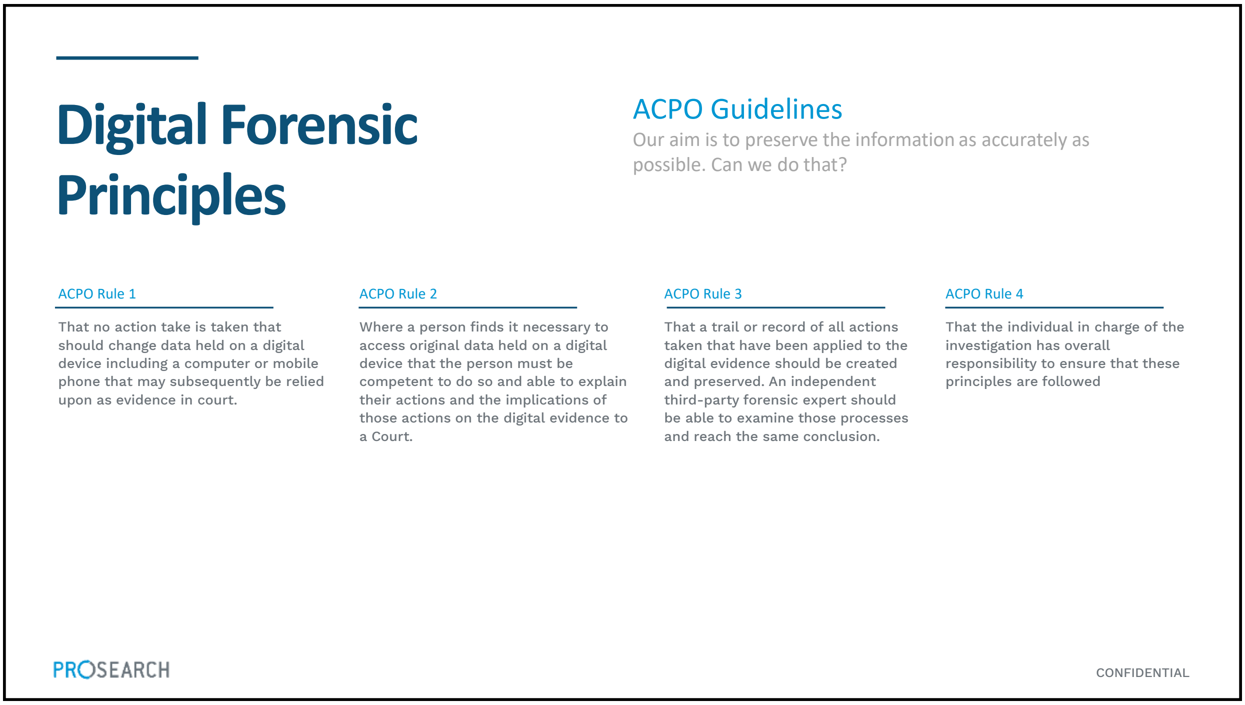


## General Forensic Process

Identification → Preservation / Collection → Examination → Analysis → Presentation

CONFIDENTIAL

5



## Digital Forensic Principles

### ACPO Guidelines

Our aim is to preserve the information as accurately as possible. Can we do that?

**ACPO Rule 1**

That no action take is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court.

**ACPO Rule 2**

Where a person finds it necessary to access original data held on a digital device that the person must be competent to do so and able to explain their actions and the implications of those actions on the digital evidence to a Court.

**ACPO Rule 3**

That a trail or record of all actions taken that have been applied to the digital evidence should be created and preserved. An independent third-party forensic expert should be able to examine those processes and reach the same conclusion.

**ACPO Rule 4**

That the individual in charge of the investigation has overall responsibility to ensure that these principles are followed

CONFIDENTIAL

6

# Internet Basics

7

# The anatomy of a webpage

**At Source (server side)**

A webpage can be considered as a collection of elements.

HTML is a markup language that tells the browser what elements to put where and how

- Add some text
- Reserve space for my photos which I store in a folder
- Reserve space for adverts
- Reserve space for videos. Its stored on YouTube

I send my prepared page to an ISP who gives it a webpage name and makes it available to the WWW.

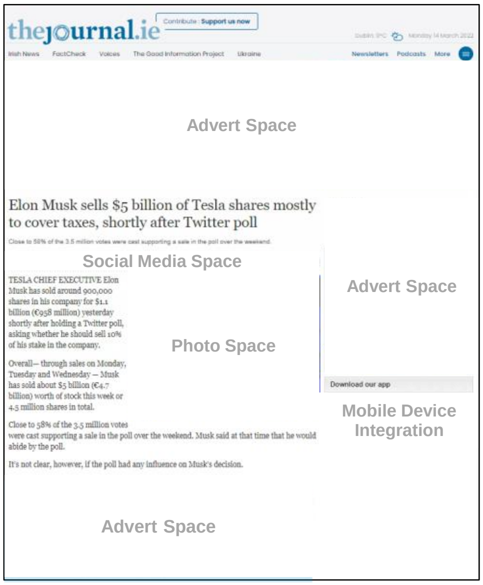
**At destination (client side)**

Users log into the webpage

The ISP server sends all elements of the webpage.

'Embedded' elements are retrieved from YouTube, Facebook etc.

**The exact final look of the page may not be known to the creator**



Elon Musk sells $5 billion of Tesla shares mostly to cover taxes, shortly after Twitter poll

Close to 58% of the 3.5 million votes were cast supporting a sale in the poll over the weekend.

TESLA CHIEF EXECUTIVE Elon Musk has sold around 900,000 shares in his company for $1.1 billion (€958 million) yesterday shortly after holding a Twitter poll, asking whether he should sell 10% of his stake in the company.

Overall– through sales on Monday, Tuesday and Wednesday – Musk has sold about $5 billion (€4.7 billion) worth of stock this week or 4.5 million shares in total.

Close to 58% of the 3.5 million votes were cast supporting a sale in the poll over the weekend. Musk said at that time that he would abide by the poll.

It's not clear, however, if the poll had any influence on Musk's decision.

PROSEARCH

CONFIDENTIAL

8

# The anatomy of a webpage

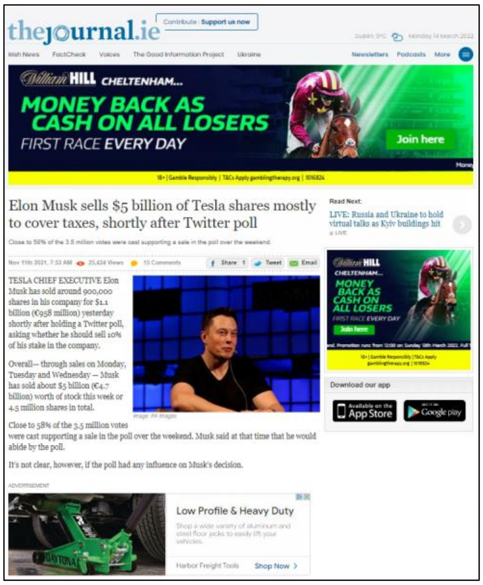
A single page is created using content from **multiple** sources and elements

**71**
# Individual **Files** making the page

**12**
Distinct **Domains** the site is connecting to

**0**
Videos Downloaded

**10**
Adverts Downloaded



thejournal.ie

Contribute : Support us now

Irish News FactCheck Voices The Good Information Project Ukraine Newsletters Podcasts More

Monday 14 March 2022

Elon Musk sells $5 billion of Tesla shares mostly to cover taxes, shortly after Twitter poll

Close to 58% of the 3.5 million votes were cast supporting a sale in the poll over the weekend.

Nov 11th 2021, 7:53 AM 25,424 Views 15 Comments Share 1 Tweet Email

TESLA CHIEF EXECUTIVE Elon Musk has sold around 900,000 shares in his company for $1.1 billion (€958 million) yesterday shortly after holding a Twitter poll, asking whether he should sell 10% of his stake in the company.

Overall— through sales on Monday, Tuesday and Wednesday — Musk has sold about $5 billion (€4.7 billion) worth of stock this week or 4.5 million shares in total.

Image: PA Images

Close to 58% of the 3.5 million votes were cast supporting a sale in the poll over the weekend. Musk said at that time that he would abide by the poll.

It's not clear, however, if the poll had any influence on Musk's decision.

Read Next:

LIVE: Russia and Ukraine to hold virtual talks as Kyiv buildings hit

Download our app

App Store Google play

ADVERTISEMENT

PROSEARCH

CONFIDENTIAL

# Webpage DNA

**HTML** is the source code of the page

It's a set of instructions to gather information and show it in the browser.

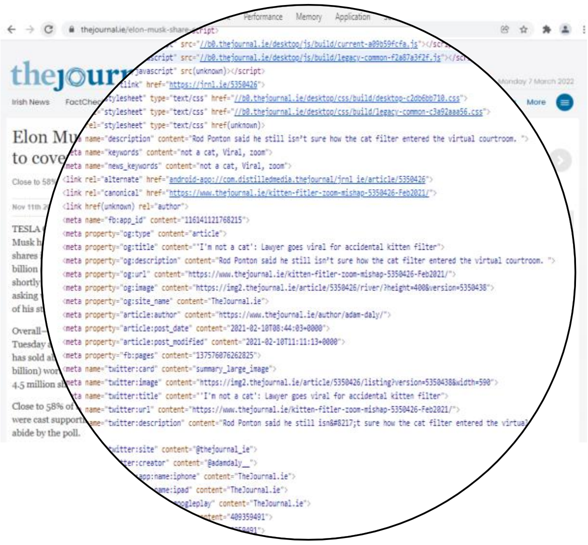
It also shows much more useful hidden information:

**Exact URLs** https://www.youtube.com/watch?v=tNRLZLK475A

**Meta tag** meta name="article:post_date" content=2021-02-10T08:44:03+000">

**Comment tag** <! – You can't see me ☺☺ -->

**'Hidden' tag** <input type="hidden">



```
script>
t" src="//b0.thejournal.ie/desktop/js/build/current-a09b59fcfa.js"></scr
ascript" src="//b0.thejournal.ie/desktop/js/build/legacy-common-f2a87a3f2f.js"></scr
javascript" src(unknown)></script>
link" href="https://jrnl.ie/5350426">
tylesheet" type="text/css" href="//b0.thejournal.ie/desktop/css/build/desktop-c2db6bb710.css">
="stylesheet" type="text/css" href="//b0.thejournal.ie/desktop/css/build/legacy-common-c3a92aaa56.css">
el="stylesheet" type="text/css" href(unknown)>
 name="description" content="Rod Ponton said he still isn't sure how the cat filter entered the virtual courtroom. ">
eta name="keywords" content="not a cat, Viral, zoom">
meta name="news_keywords" content="not a cat, Viral, zoom">
<link rel="alternate" href="android-app://com.distilledmedia.thejournal/jrnl_ie/article/5350426">
<link rel="canonical" href="https://www.thejournal.ie/kitten-fitler-zoom-mishap-5350426-Feb2021/">
<link href(unknown) rel="author">
<meta name="fb:app_id" content="116141121768215">
<meta property="og:type" content="article">
<meta property="og:title" content="'I'm not a cat': Lawyer goes viral for accidental kitten filter">
<meta property="og:description" content="Rod Ponton said he still isn't sure how the cat filter entered the virtual courtroom. ">
<meta property="og:url" content="https://www.thejournal.ie/kitten-fitler-zoom-mishap-5350426-Feb2021/">
<meta property="og:image" content="https://img2.thejournal.ie/article/5350426/river/?height=400&version=5350438">
<meta property="og:site_name" content="TheJournal.ie">
<meta property="article:author" content="https://www.thejournal.ie/author/adam-daly/">
<meta property="article:post_date" content="2021-02-10T08:44:03+0000">
<meta property="article:post_modified" content="2021-02-10T11:11:13+0000">
<meta property="fb:pages" content="137576076262825">
<meta name="twitter:card" content="summary_large_image">
meta name="twitter:image" content="https://img2.thejournal.ie/article/5350426/listing?version=5350438&width=590">
ta name="twitter:title" content="'I'm not a cat': Lawyer goes viral for accidental kitten filter">
 name="twitter:url" content="https://www.thejournal.ie/kitten-fitler-zoom-mishap-5350426-Feb2021/">
ame="twitter:description" content="Rod Ponton said he still isn&#8217;t sure how the cat filter entered the virtual
witter:site" content="@thejournal_ie">
ter:creator" content="@adamdaly__">
app:name:iphone" content="TheJournal.ie">
name:ipad" content="TheJournal.ie">
oogleplay" content="TheJournal.ie">
tent="409359491">
```

Elon Mu
to cove
Close to 58%
Nov 11th 2
TESLA
Musk h
shares
billion
shortly
asking
of his st
Overall—
Tuesday
has sold a
billion) wor
4.5 million sh
Close to 58% of
were cast support
abide by the poll.

PROSEARCH

CONFIDENTIAL

# Web 1.0 v Web 2.0 v Web3

### Web 1.0

Name given to the original use of the World Wide Web

Sites were created for the **consumption** of content

Static web pages are created by any user with web creation software

Uses: HTML \ PHP \ CSS

Personal web pages were common but simple

Services did exist to help create pages more quickly, but the primary use is of **creating, disseminating and consuming** content

Little to no user participation

### Web 2.0

A new iteration of how the web is used

Instead of a user consuming a web site's content the user is encouraged to **contribute** to make comments, edits and other participation.

Another name for Social Media, or the Social Web

The pages are developed using a more advanced technology and usually administered by dedicated platforms

Communications is secured via accounts

Accounts and participation is maintained by the service

### Web3

A relatively new concept

Instead of the data of the web being centralised to the big tech companies, the data in Web3 is decentralised and controlled by the user

Based on cryptocurrency and blockchain

It could lead to a more secure and privacy focused web

Out of scope here.

# The anatomy of a Web 2.0 page

### Templates

Rather than create a website from scratch, most providers make it simple by providing a template.

All you do is to fill in the blanks

An explosion of personal content:

- Blogs
- vBlogs
- Personal websites

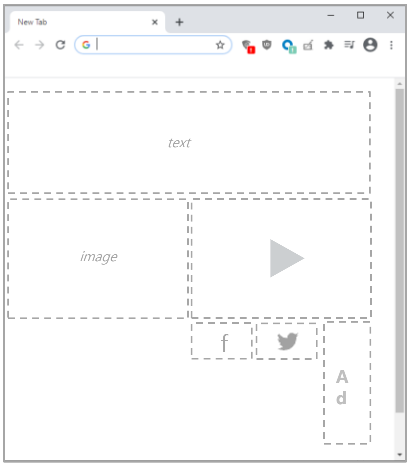
### Social Media Sites

All use some sort of a template to make the page

The elements of the pages are stored in a database.

Once they are accessed the template is sent and the database elements

**The final look is consistent. The framework of the page is the same with content different.**



# The anatomy of a Web 2.0 page

Templates

Rather than create a website from scratch, most providers make it simple by providing a template.

All you do is to fill in the blanks

An explosion of personal content:

- Blogs
- vBlogs
- Personal websites

Social Media Sites

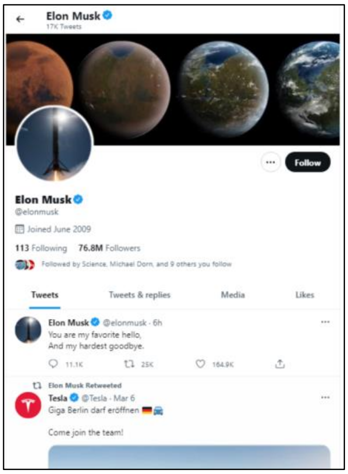
All use some sort of a template to make the page

The elements of the pages are stored in a database.

Once they are accessed the template is sent and the database elements

**The final look is consistent. The framework of the page is the same with content different.**

**The data is stored in databases. This is what we are interested in, not the templated page structure.**



Elon Musk
17K Tweets

Elon Musk
@elonmusk
Joined June 2009
113 Following 76.8M Followers
Followed by Science, Michael Dorn, and 9 others you follow

Elon Musk @elonmusk · 6h
You are my favorite hello,
And my hardest goodbye.
11.1K 25K 164.9K

Elon Musk Retweeted
Tesla @Tesla · Mar 6
Giga Berlin darf eröffnen 🇩🇪🚙

Come join the team!

PROSEARCH

CONFIDENTIAL

13

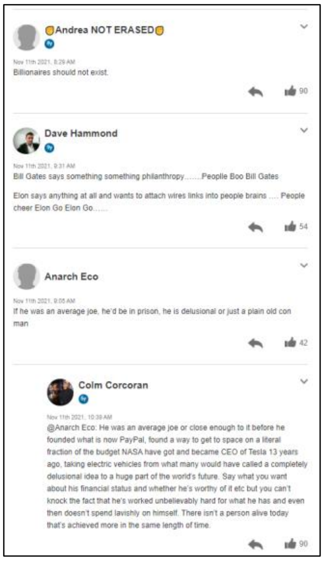
# Social Web: More than just Social Media

Social Web

Social web is the term given to the proliferation of social interaction on web sites amongst users and between sites

Examples include

- Conversations
- Comments
- Shop Reviews
- Forums
- 'Likes'



Andrea NOT ERASED
Nov 11th 2021, 8:29 AM
Billionaires should not exist.
90

Dave Hammond
Nov 11th 2021, 9:31 AM
Bill Gates says something something philanthropy.......Peoplie Boo Bill Gates

Elon says anything at all and wants to attach wires links into people brains .... People cheer Elon Go Elon Go......
54

Anarch Eco
Nov 11th 2021, 9:05 AM
If he was an average joe, he'd be in prison, he is delusional or just a plain old con man
42

Colm Corcoran
Nov 11th 2021, 10:39 AM
@Anarch Eco: He was an average joe or close enough to it before he founded what is now PayPal, found a way to get to space on a literal fraction of the budget NASA have got and became CEO of Tesla 13 years ago, taking electric vehicles from what many would have called a completely delusional idea to a huge part of the world's future. Say what you want about his financial status and whether he's worthy of it etc but you can't knock the fact that he's worked unbelievably hard for what he has and even then doesn't spend lavishly on himself. There isn't a person alive today that's achieved more in the same length of time.
90

PROSEARCH

CONFIDENTIAL

14

# General Forums

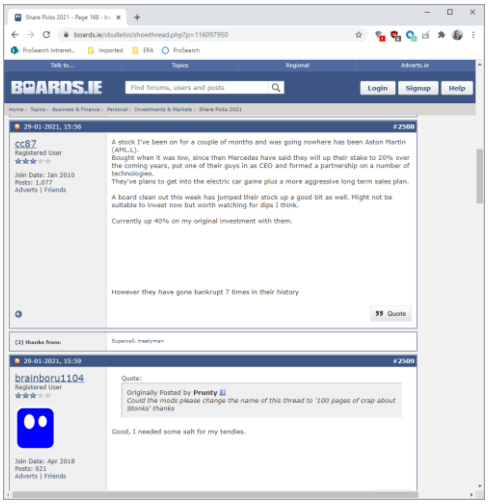
## Boards.ie

A traditional forum that allows users to discuss wider arrays of topics

- A Single users can make many threads
- A Single thread can have many posts
- A Single post can have many 'thanks' or 'likes'

A single thread can be found divided over a number of webpages.

- Each object is access via dedicated **web page URL**. The ID of that element is in the HTML and not visible to the use
- Forum software made by vBulletin


Share Picks 2021 - Page 168 - bo
boards.ie/vbulletin/showthread.php?p=116097950
ProSearch Intranet...
Imported
ERA
ProSearch
Talk to...
Topics
Regional
Adverts.ie
BOARDS.IE
Find forums, users and posts
Login
Signup
Help
Home › Topics › Business & Finance › Personal › Investments & Markets › Share Picks 2021
Quote

29-01-2021, 15:56 #2508

cc87
Registered User
Join Date: Jan 2010
Posts: 1,077
Adverts | Friends

A stock I've been on for a couple of months and was going nowhere has been Aston Martin (AML.L).
Bought when it was low, since then Mercedes have said they will up their stake to 20% over the coming years, put one of their guys in as CEO and formed a partnership on a number of technologies.
They've plans to get into the electric car game plus a more aggressive long term sales plan.

A board clean out this week has jumped their stock up a good bit as well. Might not be suitable to invest now but worth watching for dips I think.

Currently up 40% on my original investment with them.

However they have gone bankrupt 7 times in their history

(2) thanks from: Supercell, treatyman

29-01-2021, 15:59 #2509

brainboru1104
Registered User
Join Date: Apr 2018
Posts: 621
Adverts | Friends

Quote:

> Originally Posted by **Prunty**
> *Could the mods please change the name of this thread to '100 pages of crap about Stonks' thanks*

Good, I needed some salt for my tendies.

PROSEARCH

CONFIDENTIAL

15

# General Forums

## Scale

Although there are a few major social media sites with billions of users. There is far more social media data out there.

There are 4 main forum software providers

There are 100,000s of **sites** with an indeterminate amount of posts, comments etc.

| Provider | # Sites | Market Share |
|---|---|---|
| BuddyPress | 108,062 | 59.8% |
| phpBB | 18,169 | 10.05% |
| vBulletin | 15,016 | 8.31% |
| Xenforo | 10,159 | 5.62% |

PROSEARCH

CONFIDENTIAL

16

# Internet Collections

17

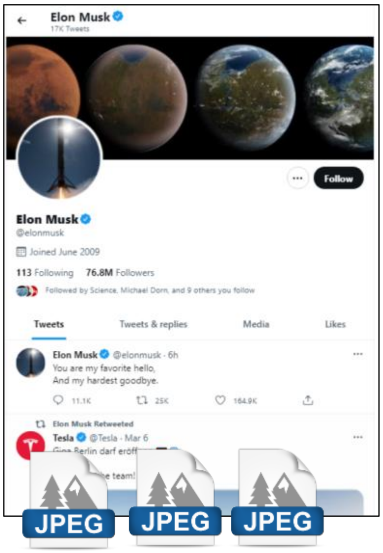
## Screenshot

### Technique

- Go to each webpage you need
- ‘Photograph’ static images of the webpages

### Problem

- Very easy to fake
- Can’t hash to compare and verify data
- Not preserving the background information (metadata)
- Need to manually browse the website which can expose your identity and affect what you see
- You may miss important information
- Slow


Elon Musk
17K Tweets

Elon Musk
@elonmusk
Joined June 2009
113 Following 76.8M Followers
Followed by Science, Michael Dorn, and 9 others you follow

Elon Musk @elonmusk · 6h
You are my favorite hello,
And my hardest goodbye.

Elon Musk Retweeted
Tesla @Tesla · Mar 6
Gina Berlin darf eröff
e team!

18

# Screencast

### Technique

- Record dynamic images, video or the behaviour
- Ensures that the content is not modified

### Problem

- Can’t hash to compare and verify data
- Not preserving the background information (metadata)
- Need to manually browse the website which can expose your identity and affect what you see
- Slow

Elon Musk
17K Tweets

Elon Musk
@elonmusk
Joined June 2009
113 Following 76.8M Followers
Followed by Science, Michael Dorn, and 9 others you follow

Elon Musk @elonmusk · 6h
You are my favorite hello,
And my hardest goodbye.
11.1K 25K 164.9K

Elon Musk Retweeted
Tesla @Tesla · Mar 6
Giga Berlin darf erö
Come join the team

# Save Webpage

### Technique

- Click Save-As to save a copy of the webpage
- Save a webpage including images, text, and the background code.

### Problem

- Dynamic elements of a webpage make verification difficult
- Does not download or save any 3rd party content (YouTube videos)
- Still have to go to every page individually
- Slow

Elon Musk
17K Tweets

Elon Musk
@elonmusk
Joined June 2009
113 Following 76.8M Followers
Followed by Science, Michael Dorn, and 9 others you follow

Elon Musk @elonmusk · 6h
You are my favorite hello,
And my hardest goodbye.
11.1K 25K 164.9K

Elon Musk Retweeted
Tesla @Tesla · Mar 6
Giga Berlin darf eröffnen
Come join th

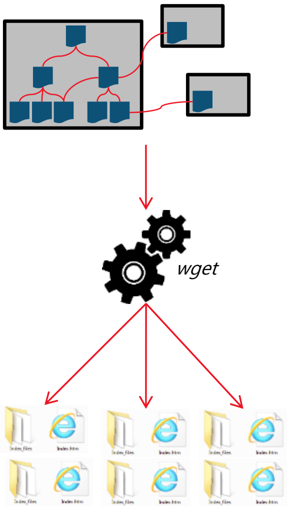
# Save Script

## Technique

- Download multiple pages all at once
- Can be tailored to follow any third-party links to download
- List the URLs to gather the lot
- Software: **wget, httrack**

## Problem

- Fairly technical to set up
- Not suitable all sites (such as social media and HTML5)
- You need to list each URL individually
- May be thousands of pages to visit



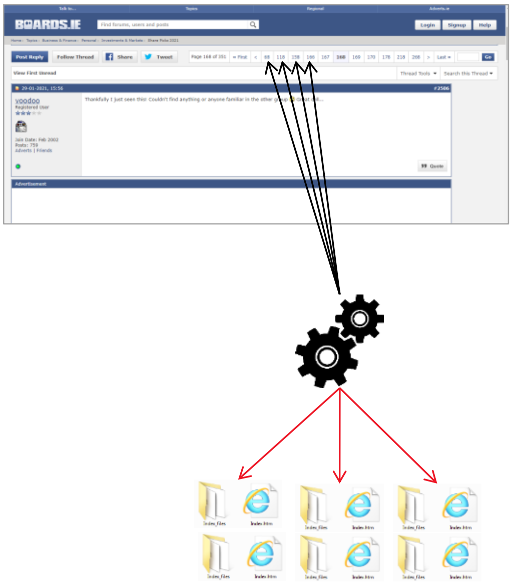
# Screen Scraping

## Technique

- Screen scraping is a technique where a tool is made to follow links just like a human would do on a page.
- Download all posts a user made as well as all of the responses for context
- Very easy analysis as well as preservation of how data looked originally

## Problem

- Software needs to be created for every type of forum <u>vendor</u>
- <u>No known software that does it all.</u>



Thankfully I just seen this! Couldn't find anything or anyone familiar in the other group 😊 Great call...

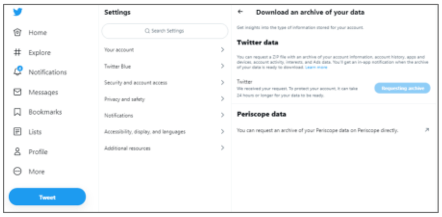
# Data Export

## Technique

- Some social media platforms have a capability to export all your media out.
- Usually very simple to do and you should get your data in a nice readable form
- Available for: LinkedIn, Facebook, Twitter

## Problem

- You need the credentials of the user to do this
- You are trusting the social network to extract a complete history
- Not available for most social web sites (Reddit, Boards.ie etc)
- The Data Source dictates HOW the data is exported. Some sources export their data in a series of PDFs which are difficult to review.
- Facebook export a mini website whcih is difficult to search



Settings

Search Settings

Your account
Twitter Blue
Security and account access
Privacy and safety
Notifications
Accessibility, display, and languages
Additional resources

Download an archive of your data

Get insights into the type of information stored for your account.

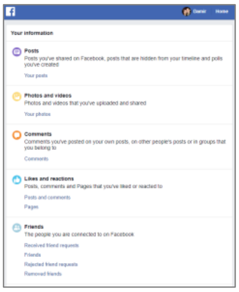
Twitter data

You can request a ZIP file with an archive of your account information, account history, apps and devices, account activity, interests, and Ads data. You'll get an in-app notification when the archive of your data is ready to download. Learn more

Twitter
We received your request. To protect your account, it can take 24 hours or longer for your data to be ready.
Requesting archive

Periscope data

You can request an archive of your Periscope data on Periscope directly.



Your information

Posts
Posts you've shared on Facebook, posts that are hidden from your timeline and polls you've created
Your posts

Photos and videos
Photos and videos that you've uploaded and shared
Your photos

Comments
Comments you've posted on your own posts, on other people's posts or in groups that you belong to
Comments

Likes and reactions
Posts, comments and Pages that you've liked or reacted to
Posts and comments
Pages

Friends
The people you are connected to on Facebook
Received friend requests
Friends
Rejected friend requests
Removed friends

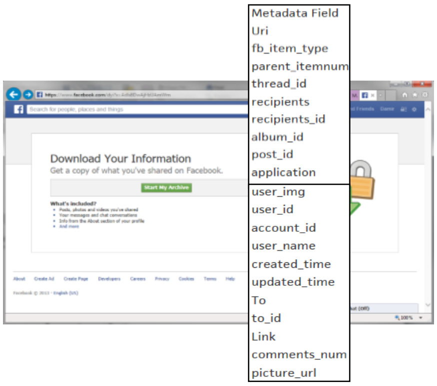
# APIs

## Technique

- Most Social Media platforms publish APIs and support protocols to allow software to connect and read data
- Collects much more than can be seen
- Can be automated easily
- Commercial professional tools exist

## Problem

- Not all vendors support these functions
- APIs can be changed at any time without notice


https://www.facebook.com/dyi?x=AdkBDwAjHzUAmWm
Search for people, places and things
Find Friends
Damir
Chat (Off)
100%

Download Your Information
Get a copy of what you've shared on Facebook.
Start My Archive

What's included?
- Posts, photos and videos you've shared
- Your messages and chat conversations
- Info from the About section of your profile
- And more

About Create Ad Create Page Developers Careers Privacy Cookies Terms Help
Facebook © 2013 · English (US)

| Metadata Field |
|---|
| Uri |
| fb_item_type |
| parent_itemnum |
| thread_id |
| recipients |
| recipients_id |
| album_id |
| post_id |
| application |
| user_img |
| user_id |
| account_id |
| user_name |
| created_time |
| updated_time |
| To |
| to_id |
| Link |
| comments_num |
| picture_url |

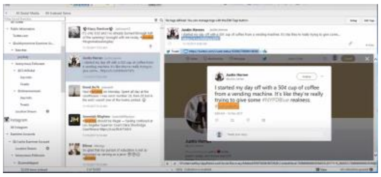
X1 DISCOVERY
RE SOFTWA INVESTIGATIVE TOOLS
AF W Professional

# APIs

X1 Discovery

- Supports: Twitter, Instagram, Facebook, Tumblr, YouTube and Online mail
- Downloads all components, hashes the files and maintains an audit trail

X1 DISCOVERY



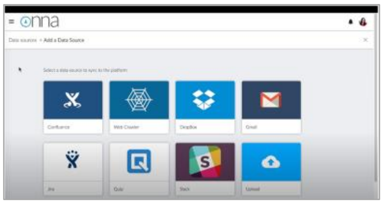
Magnet AXIOM

- Full fledged forensics software
- Support collections from Facebook only

Onna

- Supports Teams, Slack, Twitter, Confluence, Jira, Box, OneDrive, Sharepoint, etc.
- Download all accessible information and presents it in a usable fashion

onna



onna
Data sources > Add a Data Source
Select a data source to sync to the platform
Confluence
Web Crawler
DropBox
Gmail
Jira
Quip
Slack
Upload

Page Freezer

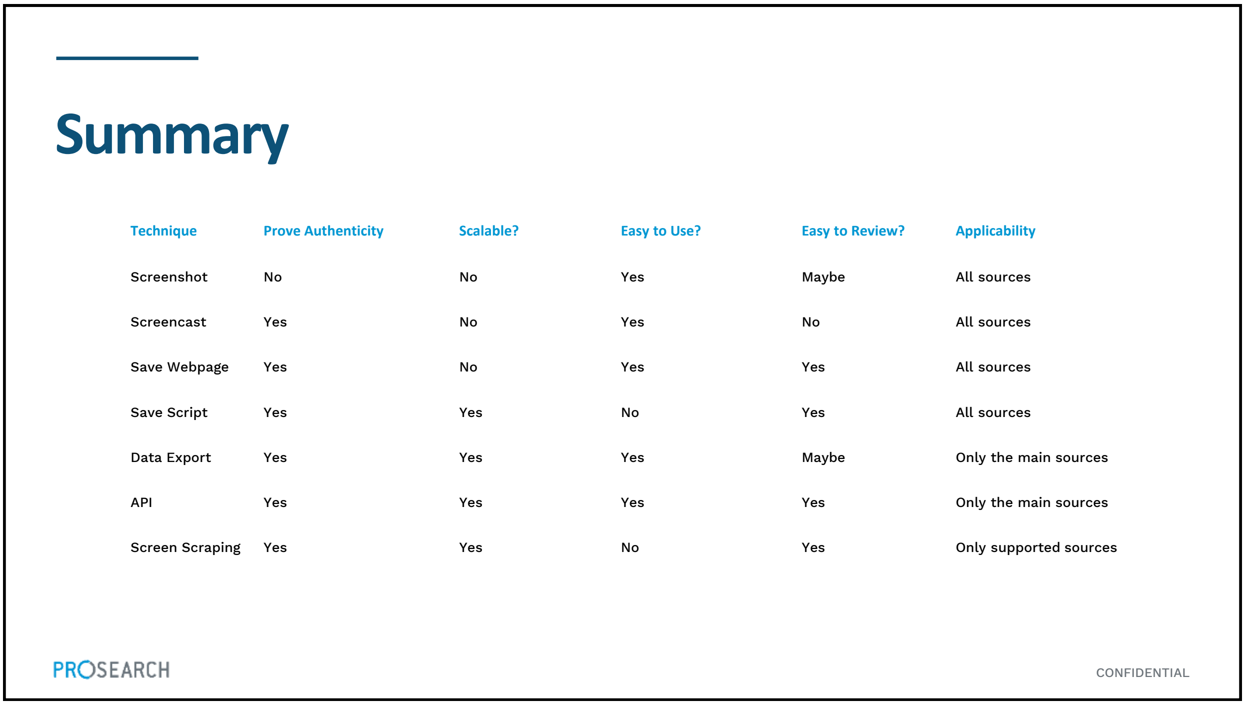
PROSEARCH CONFIDENTIAL

25

# DEMO

PROSEARCH CONFIDENTIAL

26



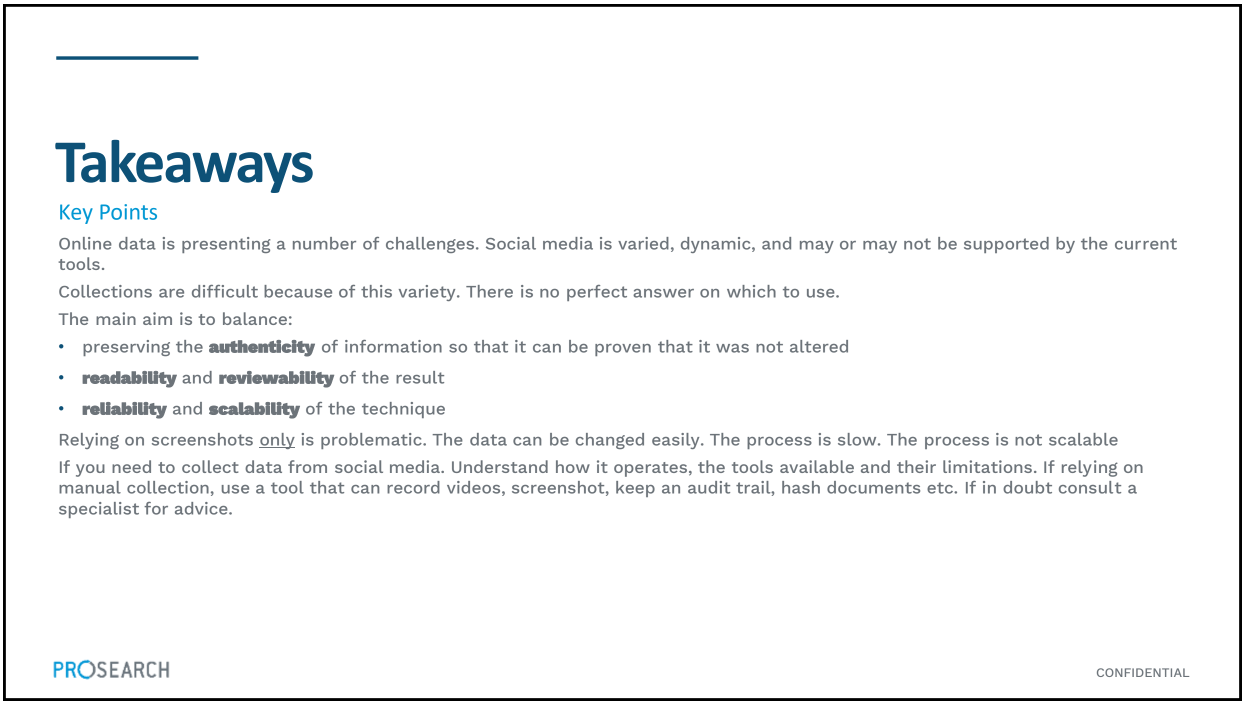
# Summary

| Technique | Prove Authenticity | Scalable? | Easy to Use? | Easy to Review? | Applicability |
|---|---|---|---|---|---|
| Screenshot | No | No | Yes | Maybe | All sources |
| Screencast | Yes | No | Yes | No | All sources |
| Save Webpage | Yes | No | Yes | Yes | All sources |
| Save Script | Yes | Yes | No | Yes | All sources |
| Data Export | Yes | Yes | Yes | Maybe | Only the main sources |
| API | Yes | Yes | Yes | Yes | Only the main sources |
| Screen Scraping | Yes | Yes | No | Yes | Only supported sources |

PROSEARCH

CONFIDENTIAL

27



# Takeaways

## Key Points

Online data is presenting a number of challenges. Social media is varied, dynamic, and may or may not be supported by the current tools.

Collections are difficult because of this variety. There is no perfect answer on which to use.

The main aim is to balance:

- preserving the **authenticity** of information so that it can be proven that it was not altered
- **readability** and **reviewability** of the result
- **reliability** and **scalability** of the technique

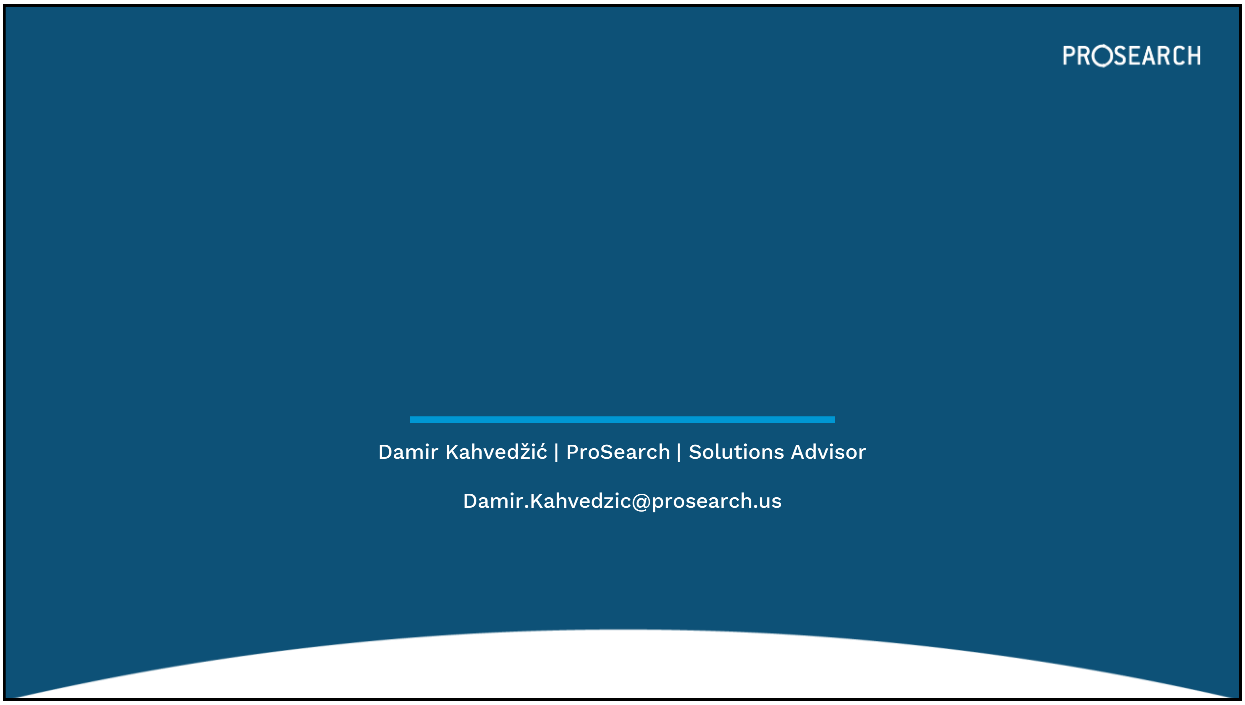
Relying on screenshots only is problematic. The data can be changed easily. The process is slow. The process is not scalable

If you need to collect data from social media. Understand how it operates, the tools available and their limitations. If relying on manual collection, use a tool that can record videos, screenshot, keep an audit trail, hash documents etc. If in doubt consult a specialist for advice.

PROSEARCH

CONFIDENTIAL

28



PROSEARCH

Damir Kahvedžić | ProSearch | Solutions Advisor

Damir.Kahvedzic@prosearch.us

29

# Academy of European Law

## Obtaining e-evidence when investigating and prosecuting crimes /Cracow, 24-25 March 2022/

## Examination of digital devices

Anna ILLAMAA, anna.illamaa@gmail.com

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

1

Anna ILLAMAA

Estonian Police and Border Guard Board

National Police, Digital Forensic Centre

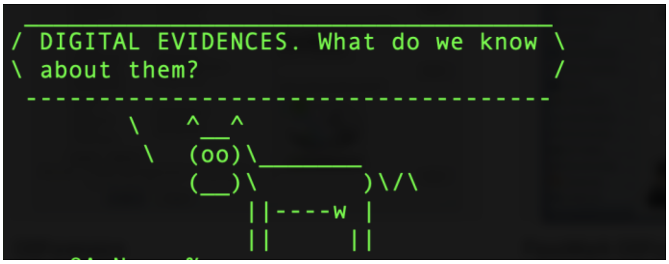
Estonian Police and Border Guard Board

2

## Topics

- Windows, macOS, Linux artefacts
  - File systems

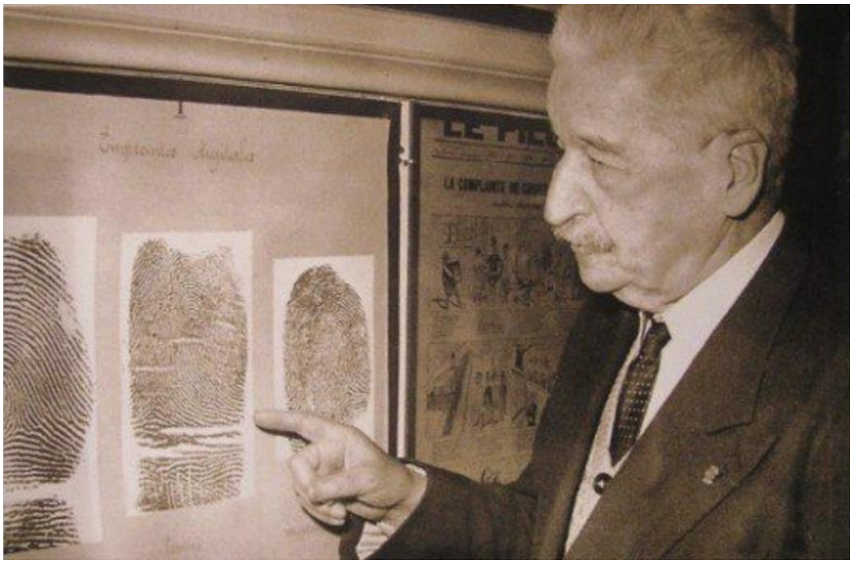
- Digital evidences handling
  - Methodology
  - Chain on custody



```
 ____________________________________
/ DIGITAL EVIDENCES. What do we know \
\ about them?                        /
 ------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

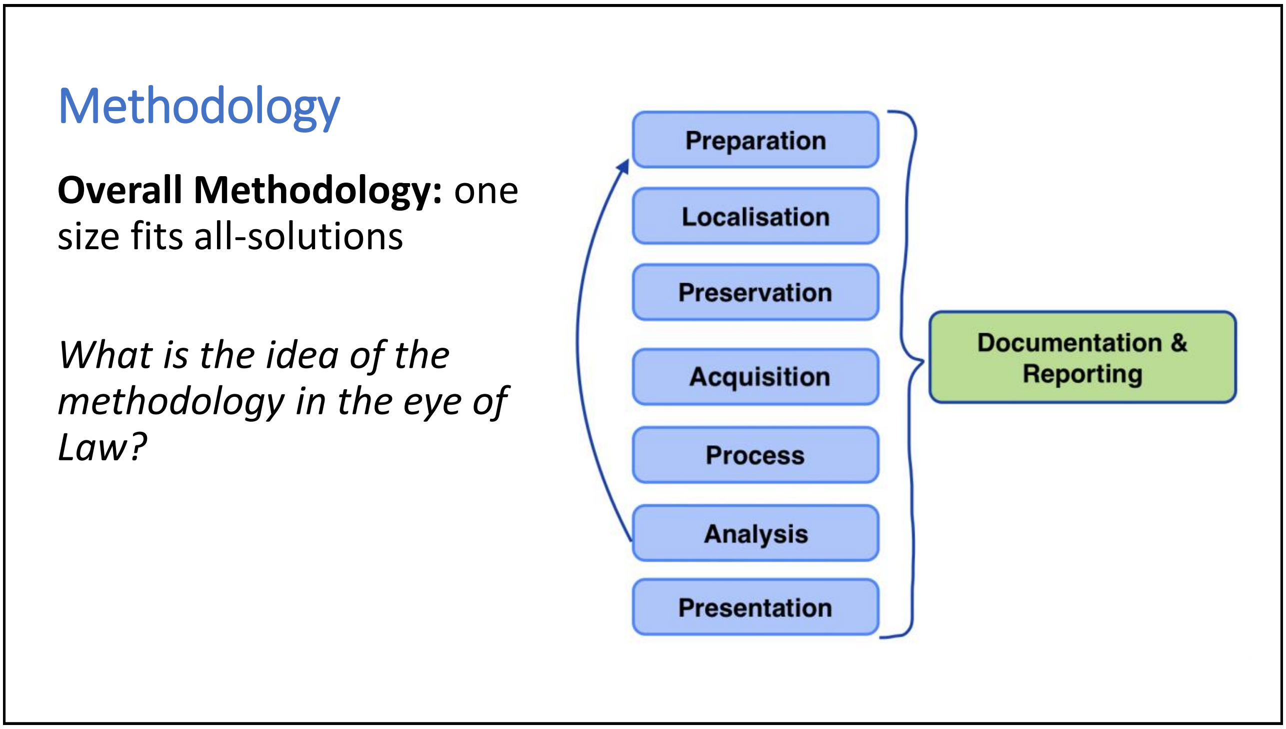
3

Edmond Locard, Sherlock Holmes of France



“Every contact leaves a trace”

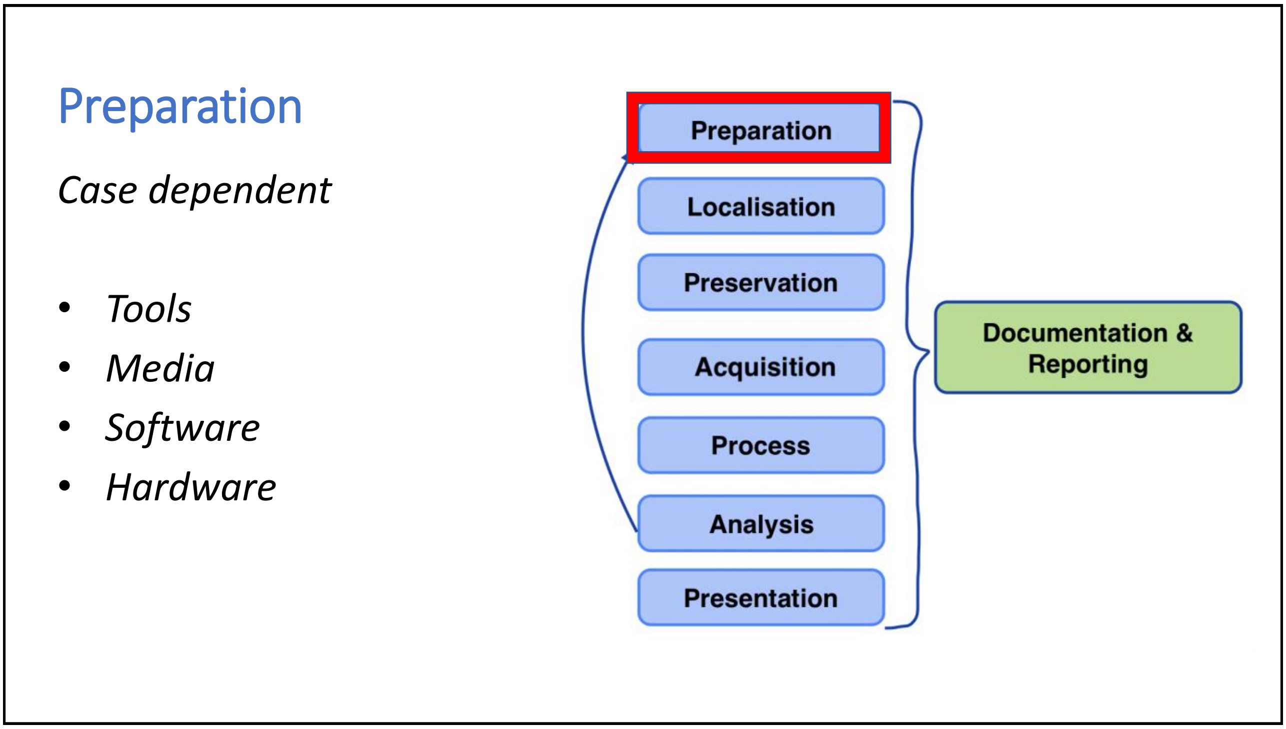
4



## Methodology

**Overall Methodology:** one size fits all-solutions

*What is the idea of the methodology in the eye of Law?*



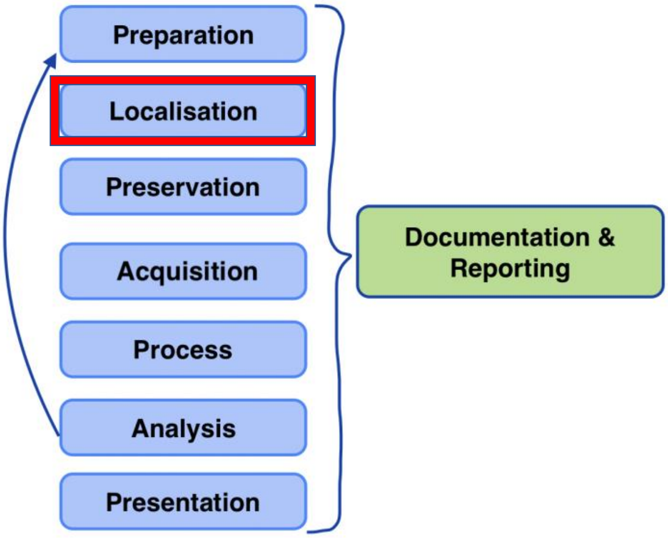
## Preparation

*Case dependent*

- *Tools*
- *Media*
- *Software*
- *Hardware*

## Localisation

- *Where you have found the devices*
- *Circumstances*
- *Taking pictures or video*



Preparation

Localisation

Preservation

Acquisition

Process

Analysis

Presentation

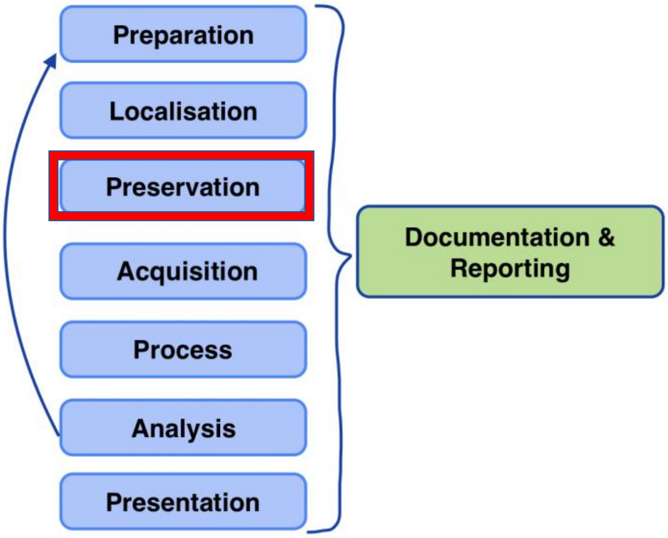
Documentation & Reporting

7

## Preservation

- *Packaging*
  - physical shock and electromagnetism
- *Tagging*

This is the starting point of the *Chain of Custody*!



Preparation

Localisation

Preservation

Acquisition

Process

Analysis

Presentation

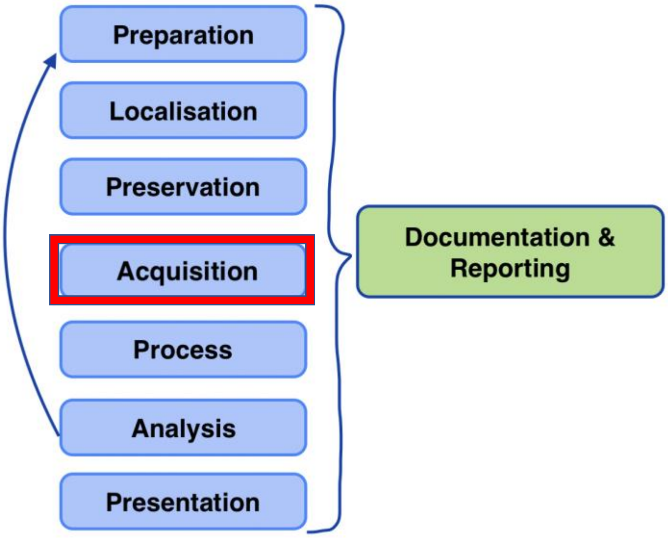
Documentation & Reporting

8

## Acquisition

*Aka <disk imaging>*

- *at the crime scene*
- *in a forensic lab*
- *software*
- *hardware*

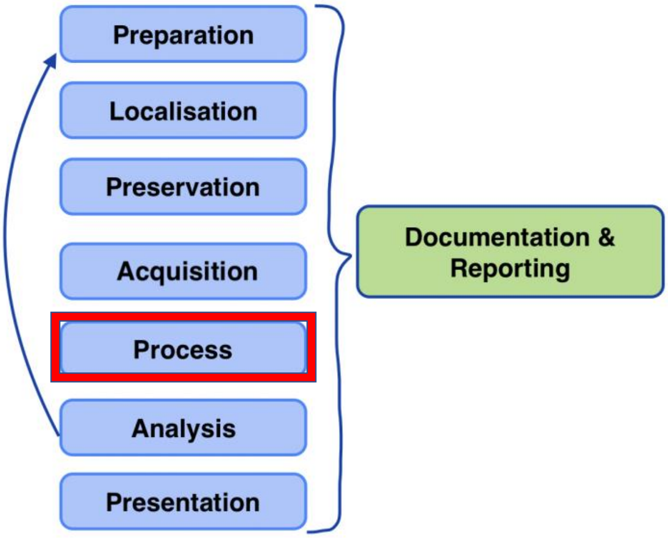


9

## Process

*last preparations before analysis*

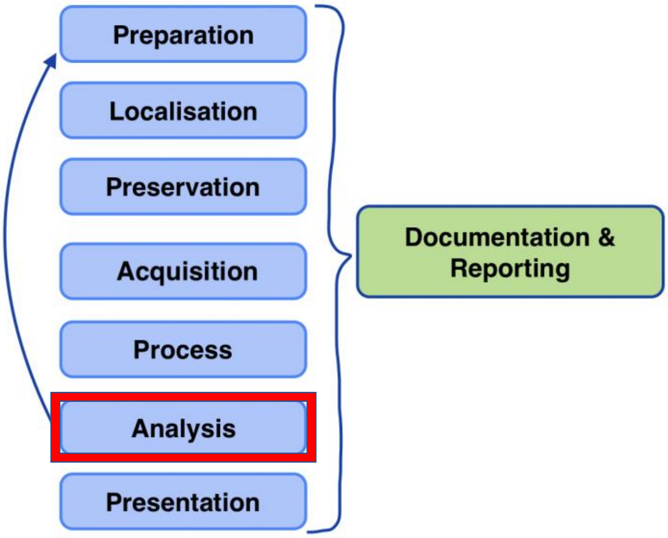
- *Decrypting*
- *Recovering*
- *Extracting*



10

## Analysis

- *open mind*
- *evidence which not only proves guilt of a suspect, but also the evidence which proves innocence*
- *verification*



Preparation

Localisation

Preservation

Acquisition

Process

Analysis

Presentation

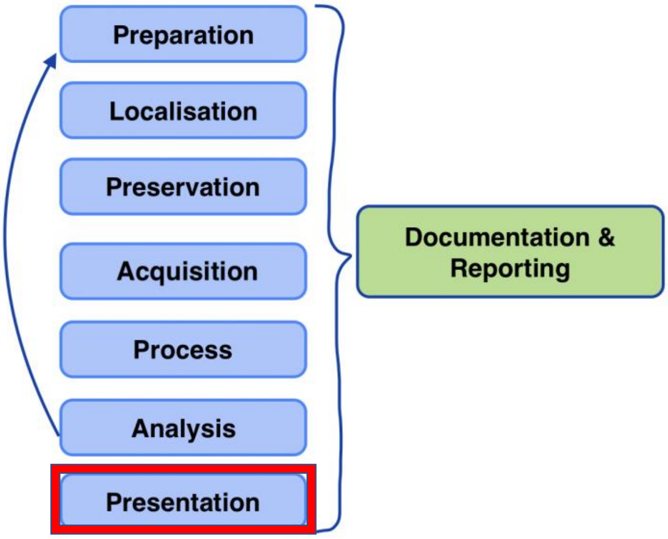
Documentation & Reporting

11

## Presentation

*Report*

- *layman language*
- *open and* clear



Preparation

Localisation

Preservation

Acquisition

Process

Analysis

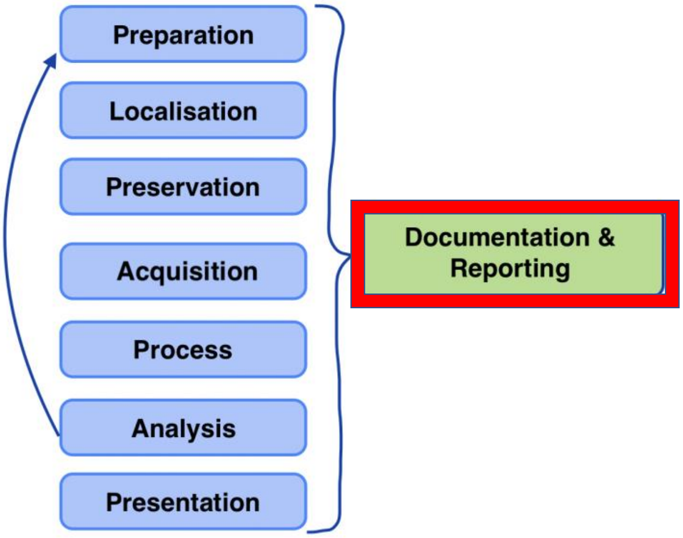
Presentation

Documentation & Reporting

12

## Documentation

- *Integration into the process*
- *During the all stages*
- *Recreation of process and findings*



Preparation

Localisation

Preservation

Acquisition

Process

Analysis

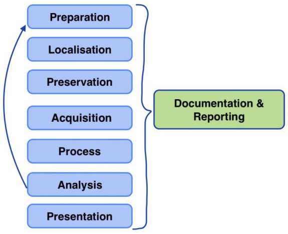
Presentation

Documentation & Reporting

13

## CASE

An employee is suspected of stealing a USB stick containing confidential information. Our task is to pay the suspect a visit and look for the USB stick. If found, verify that it contains the confidential information. We are asked not to visually read the content of the files. The employer has provided a description of the stick



Preparation

Localisation

Preservation

Acquisition

Process

Analysis

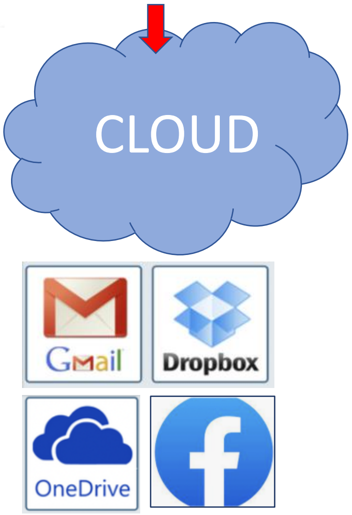
Presentation

Documentation & Reporting

14

## Sources of Digital Evidence

**Physical Devices - Data related to a person - Other**



Pay
0000 0000 0000
00/00
CCTV

15

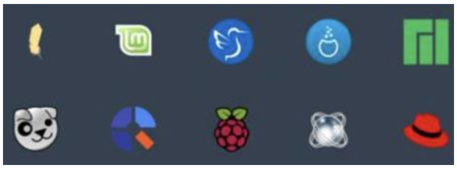
## Operating system

- is the main controlling software between the computer hardware and the user

- Windows
- macOS
- Linux/Unix

Windows1 1985
Windows 3.1 1992
Windows 95 1995
Windows XP 2001
Windows Vista 2006
Windows 7 2009
Windows 8 2012
Windows 10 2015

source: www.edureka.co



source: www.uhacc.org

Cheetah
Puma
Jaguar
Panther
Tiger
Leopard
Snow Leopard
Lion
Mountain Lion
Mavericks
Yosemite
El Capitan
Sierra
High Sierra
Mojave
Catalina
Big Sur
Monterey

source:www.deepakkeswani.com

16

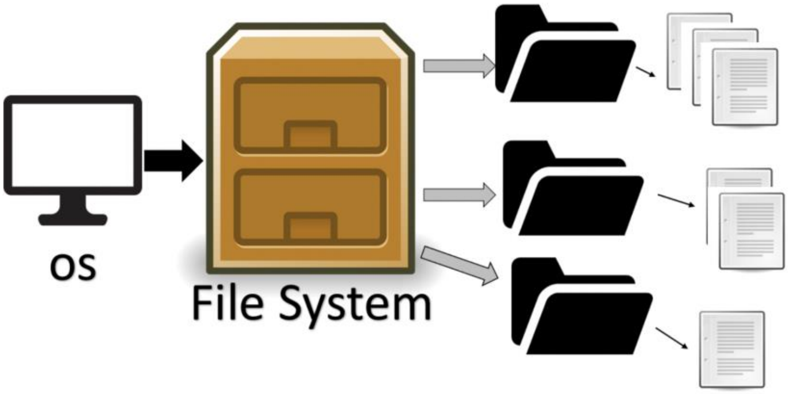
## Operating system forensics

- process of retrieving useful information from the Operating System (OS) of the computer or mobile device in question. The aim of collecting this information is to locate and acquire important information for the criminal case. We have to remember, that acquired data may prove or disprove crime and the task of forensics examiner is to establish the facts and not assumptions.

17

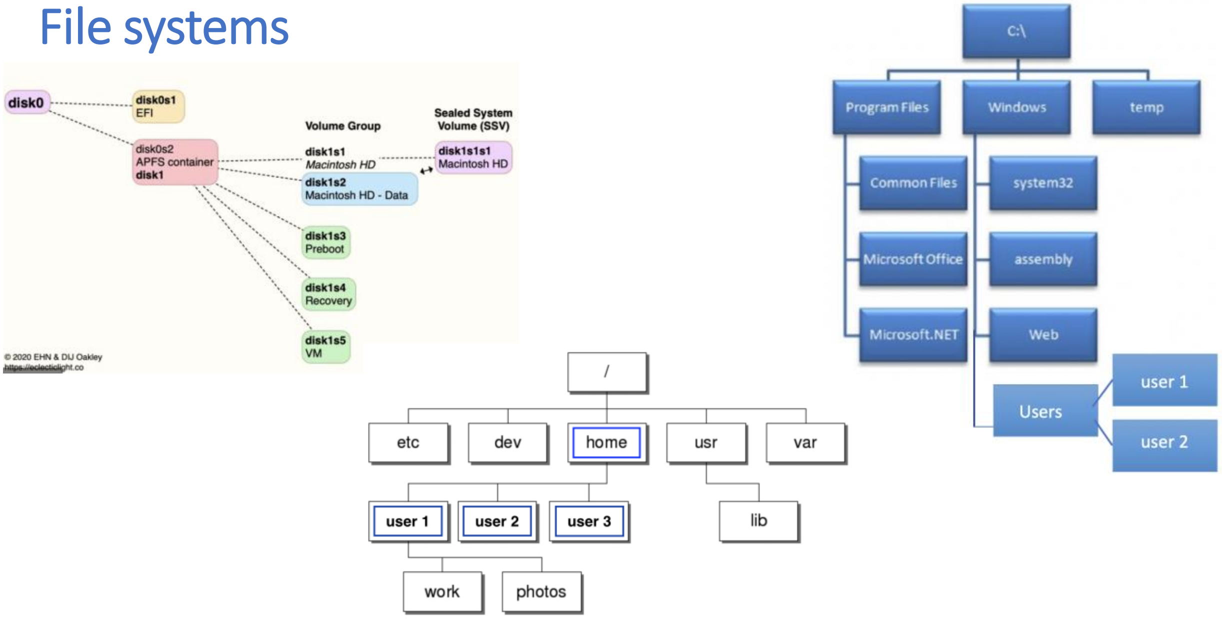
## File system

- is a method of organizing files on physical media, such as hard disks, CD's, and flash drives



18

## File systems



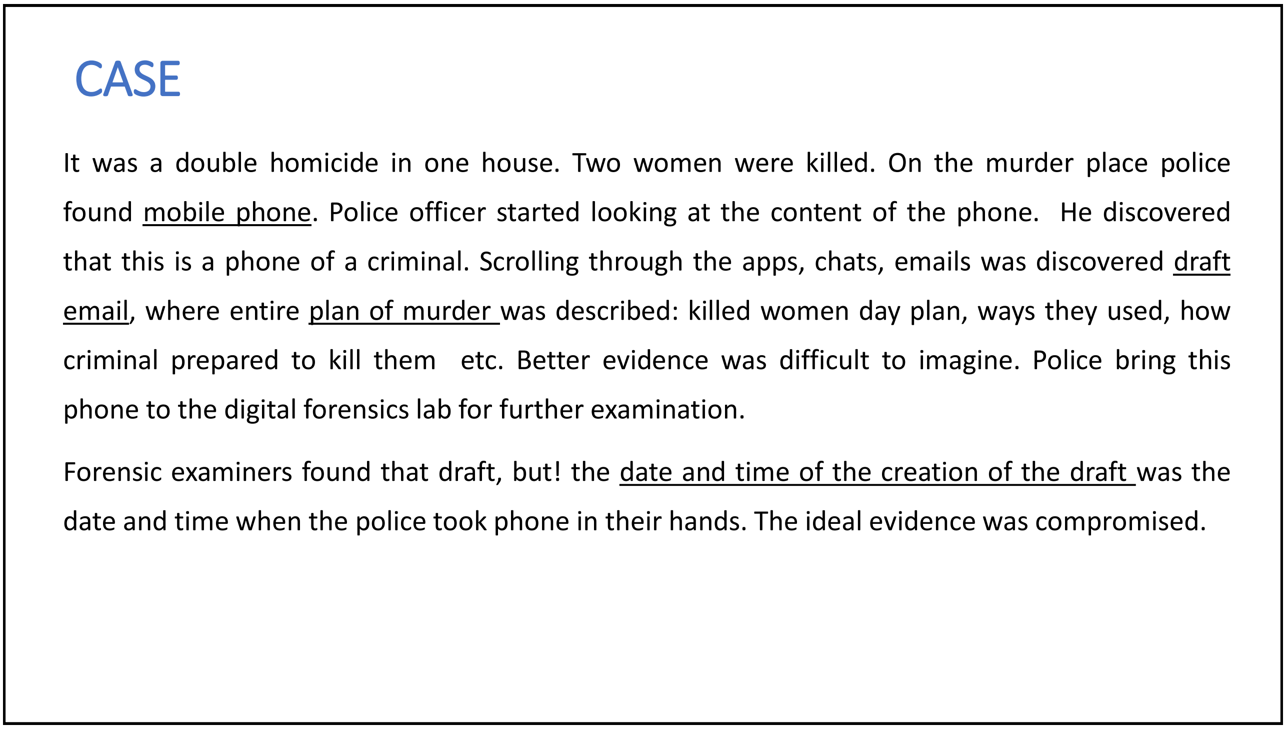
19

## Forensics Artifacts

- are objects that have forensic value

| Windows | macOS | Linux |
|---|---|---|
| Recycle Bin | Trash | Trash |
| Recent | plist | User account information |
| Registry | DS_Stores | App configuration |
| Thumbs.db | FSEvents | App and security logs |
| Print Spooling | | |

20

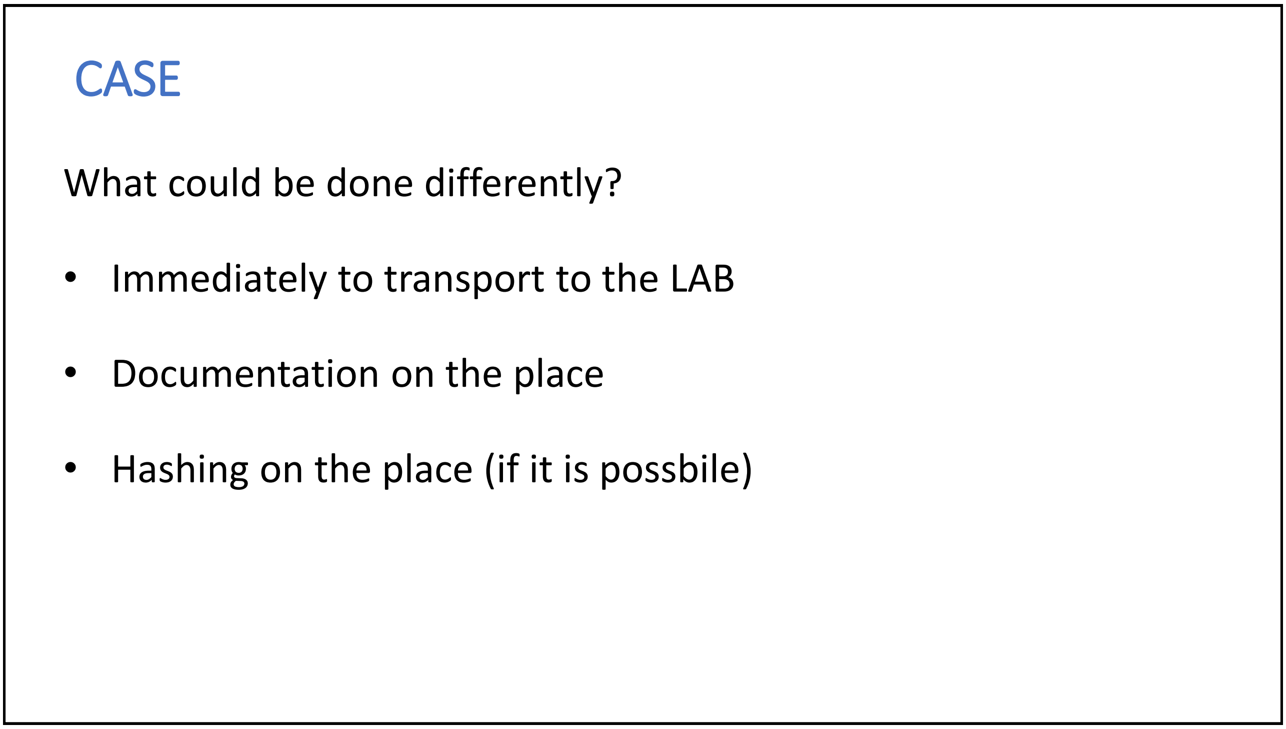


## CASE

It was a double homicide in one house. Two women were killed. On the murder place police found mobile phone. Police officer started looking at the content of the phone. He discovered that this is a phone of a criminal. Scrolling through the apps, chats, emails was discovered draft email, where entire plan of murder was described: killed women day plan, ways they used, how criminal prepared to kill them etc. Better evidence was difficult to imagine. Police bring this phone to the digital forensics lab for further examination.

Forensic examiners found that draft, but! the date and time of the creation of the draft was the date and time when the police took phone in their hands. The ideal evidence was compromised.

21



## CASE

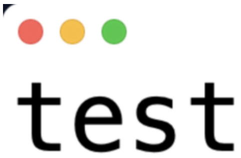
What could be done differently?

- Immediately to transport to the LAB
- Documentation on the place
- Hashing on the place (if it is possbile)

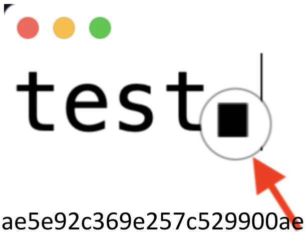
22

## Hashing

- It can't be predicted
- no two files can have the same hash value
- if the file changes, the hash value changes



test



test

SHA1: 4e1243bd22c66e76c2ba9eddc1f91394e57f9f83

SHA1: 4a4d9ae5e92c369e257c529900ae3f7ff54a7cf4

23

## We have discussed:

- Methodology
- Sources of digital evidences, handling, chain of custody
- OS, FS and artifacts
- Hashing
- Cases
- Questions?

24

# Thank you for your attention!

Anna ILLAMAA, *anna.illamaa@gmail.com*

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

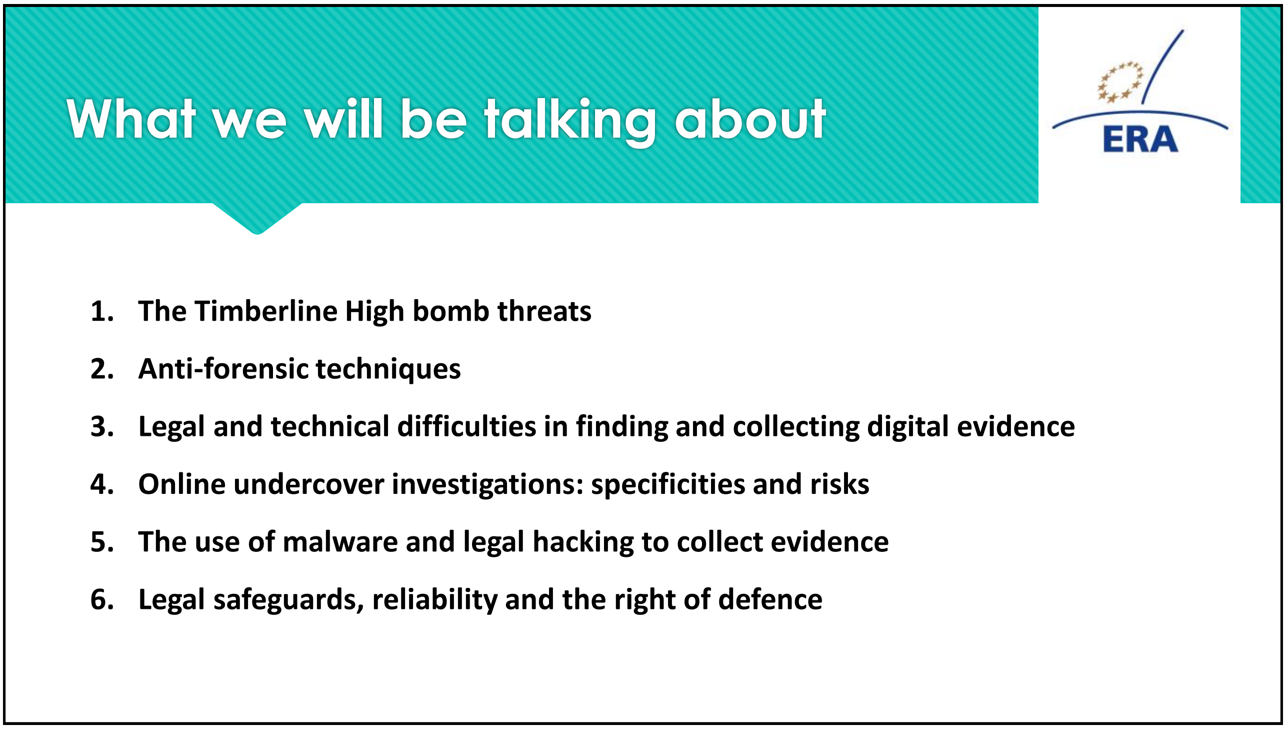
# Covert internet investigations online and legal hacking by law enforcement

**David Silva Ramalho** – dsramalho@mlgts.pt

**Lawyer** – Morais Leitão, Galvão Teles, Soares da Silva & Associados

**Assistant Teacher** – University of Lisbon's Faculty of Law

1



## What we will be talking about

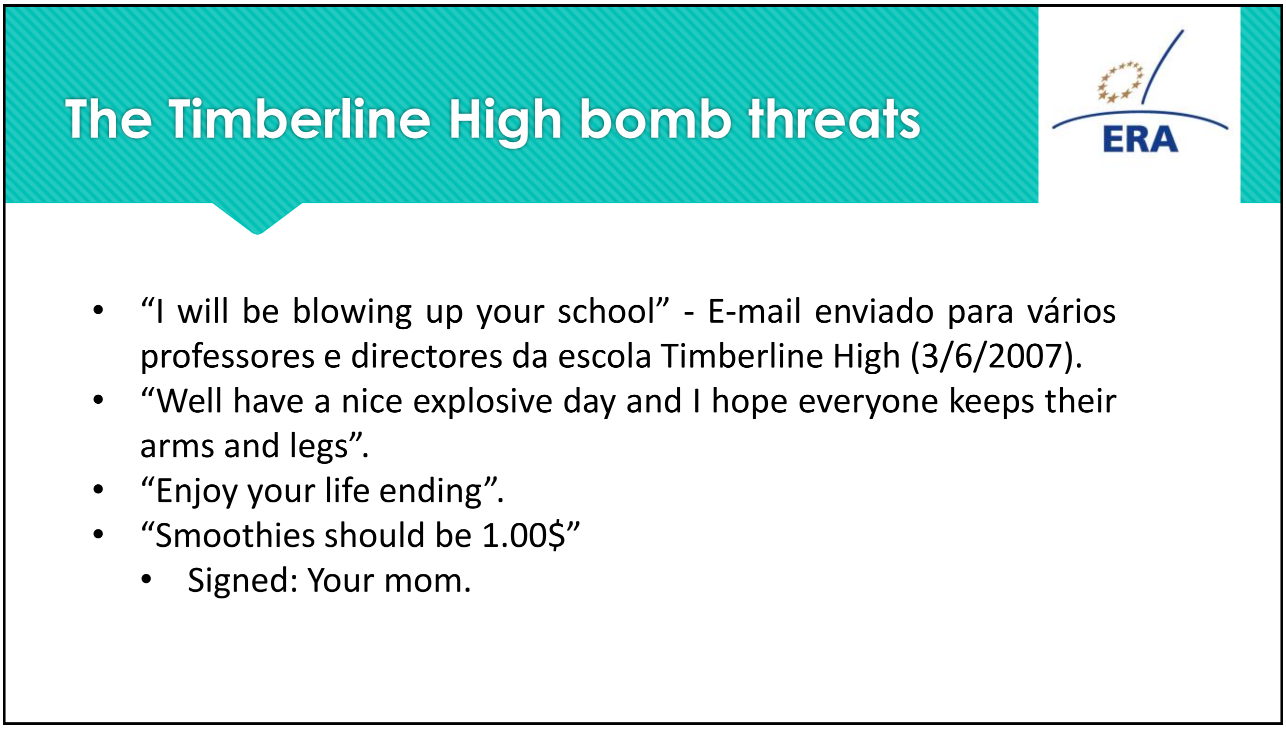
1. **The Timberline High bomb threats**
2. **Anti-forensic techniques**
3. **Legal and technical difficulties in finding and collecting digital evidence**
4. **Online undercover investigations: specificities and risks**
5. **The use of malware and legal hacking to collect evidence**
6. **Legal safeguards, reliability and the right of defence**

2

# The Timberline high bomb threats

"Have a nice exploding day"

3



## The Timberline High bomb threats

- "I will be blowing up your school" - E-mail enviado para vários professores e directores da escola Timberline High (3/6/2007).
- "Well have a nice explosive day and I hope everyone keeps their arms and legs".
- "Enjoy your life ending".
- "Smoothies should be 1.00$"
  - Signed: Your mom.

4

## The Timberline High bomb threats

- Maybe you should hire Bill Gates to tell you that [this e-mail] is coming from Italy. HAHAHA Oh wait I already told you that. So stop pretending to be “tracing it” because I have already told you it’s coming from Italy. That is where any trace will stop so just stop trying. Oh and this email will be behind a proxy behind the Italy server” (5/6/2007)

5

## The Timberline High bomb threats

- Use of at least 4 diferente Gmail accounts (incluindo thisisfromitaly@gmail.com).
- IPs from Italy and Czech Republic(proxies).
- He created a Myspace page named ‘Timberlinebombinfo«.
- The FBI was called.

6

## The Timberline High bomb threats

- Following an unsuccessful attempt to reach the “bomber”, the following e-mail was sent:
  - I respect that you do not want to be bothered by the Press. Please let me explain my actions. I am not trying to find out your true identity. As a member of the Press, I would rather not know who you are as writers are not allowed to reveal their sources. The school has continually requested that the Press NOT cover this story. After the School Meeting last night, it is obvious to me that this needs coverage. Readers find this type of story fascinating. People don’t understand your actions and we are left to guess what message you are trying to send. . . .

7

## The Timberline High bomb threats

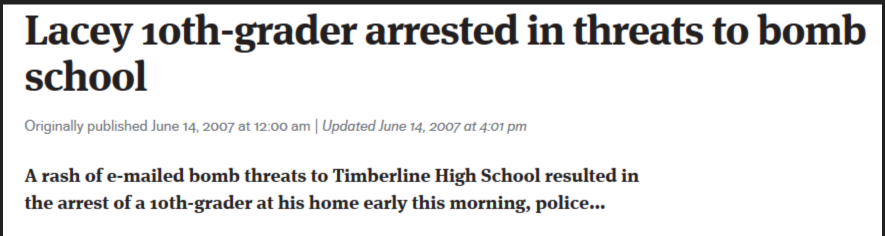
- The answer: “how can I help?”
- At 3h30 AM the suspect clicked the link infected with CIPAV.
  - It did not work
- Às 5h07 PM they began chatting in Gmail.
- 5h50 PM – A link was sent for the suspect to choose the pictures that would illustrate the article.
- 5h54 PM – “don’t care about which pics you use”. He clicked on the link. The CIPAV worked.

8

## The Timberline High bomb threats

- At 2h00 AM of June, 14 a search was made at the suspect’s house.
- They arrested, Josh G., a 15 yo 10th grade student.

9

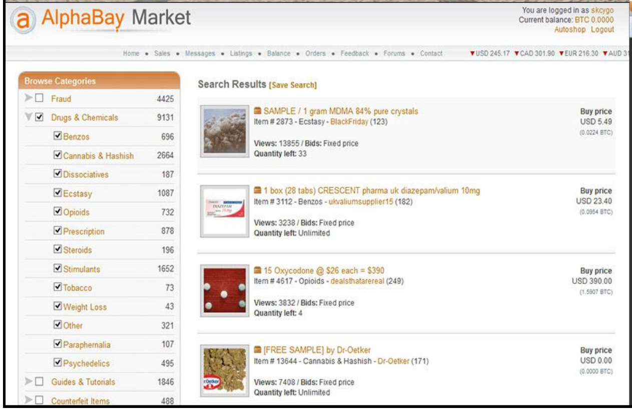


### Lacey 10th-grader arrested in threats to bomb school

Originally published June 14, 2007 at 12:00 am | *Updated June 14, 2007 at 4:01 pm*

**A rash of e-mailed bomb threats to Timberline High School resulted in the arrest of a 10th-grader at his home early this morning, police…**

10


AlphaBay Market

You are logged in as skcygo
Current balance: BTC 0.0000
Autoshop Logout

Home • Sales • Messages • Listings • Balance • Orders • Feedback • Forums • Contact ▼USD 245.17 ▼CAD 301.90 ▼EUR 216.30 ▼AUD 31

Browse Categories

| | |
|---|---|
| □ Fraud | 4425 |
| ☑ Drugs & Chemicals | 9131 |
| ☑ Benzos | 696 |
| ☑ Cannabis & Hashish | 2664 |
| ☑ Dissociatives | 187 |
| ☑ Ecstasy | 1087 |
| ☑ Opioids | 732 |
| ☑ Prescription | 878 |
| ☑ Steroids | 196 |
| ☑ Stimulants | 1652 |
| ☑ Tobacco | 73 |
| ☑ Weight Loss | 43 |
| ☑ Other | 321 |
| ☑ Paraphernalia | 107 |
| ☑ Psychedelics | 495 |
| □ Guides & Tutorials | 1846 |
| □ Counterfeit Items | 488 |

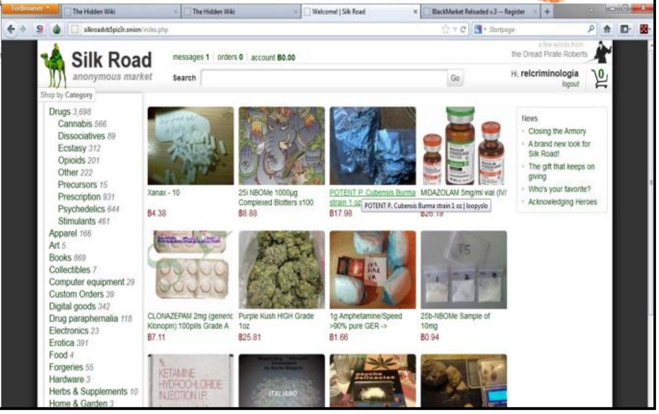
Search Results [Save Search]

SAMPLE / 1 gram MDMA 84% pure crystals
Item # 2873 - Ecstasy - BlackFriday (123)
Views: 13855 / Bids: Fixed price
Quantity left: 33
Buy price USD 5.49 (0.0224 BTC)

1 box (28 tabs) CRESCENT pharma uk diazepam/valium 10mg
Item # 3112 - Benzos - ukvaliumsupplier15 (182)
Views: 3238 / Bids: Fixed price
Quantity left: Unlimited
Buy price USD 23.40 (0.0954 BTC)

15 Oxycodone @ $26 each = $390
Item # 4617 - Opioids - dealsthatarereal (249)
Views: 3832 / Bids: Fixed price
Quantity left: 4
Buy price USD 390.00 (1.5907 BTC)

[FREE SAMPLE] by Dr-Oetker
Item # 13644 - Cannabis & Hashish - Dr-Oetker (171)
Views: 7408 / Bids: Fixed price
Quantity left: Unlimited
Buy price USD 0.00 (0.0000 BTC)



Silk Road
anonymous market

messages 1 | orders 0 | account B0.00

Search Go

a few words from the Dread Pirate Roberts

Hi, relcriminologia
logout

Shop by Category

- Drugs 3,698
  - Cannabis 566
  - Dissociatives 89
  - Ecstasy 312
  - Opioids 201
  - Other 222
  - Precursors 15
  - Prescription 931
  - Psychedelics 644
  - Stimulants 461
- Apparel 166
- Art 5
- Books 869
- Collectibles 7
- Computer equipment 29
- Custom Orders 39
- Digital goods 342
- Drug paraphernalia 118
- Electronics 23
- Erotica 391
- Food 4
- Forgeries 55
- Hardware 3
- Herbs & Supplements 10
- Home & Garden 3

Xanax - 10
B4.38

25i NBOMe 1000µg Complexed Blotters x100
B8.88

POTENT P. Cubensis Burma strain 1 oz
POTENT P. Cubensis Burma strain 1 oz | loopyslo
B17.98

MIDAZOLAM 5mg/ml vial (IV/
B26.19

CLONAZEPAM 2mg (generic Klonopin):100pills Grade A
B7.11

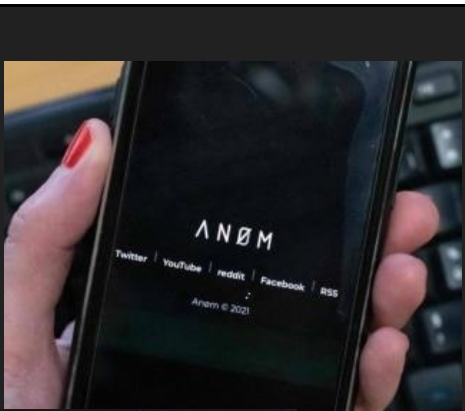
Purple Kush HIGH Grade 1oz
B25.81

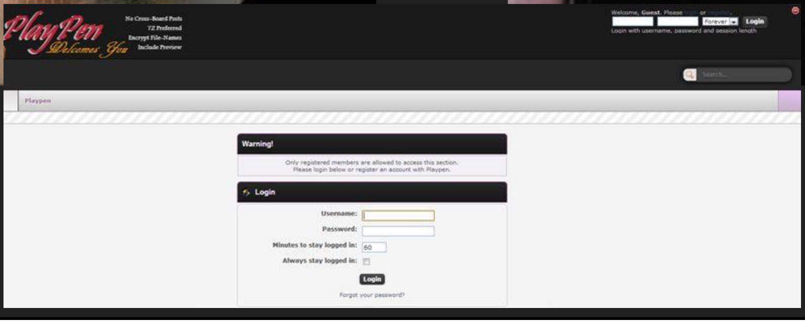
1g Amphetamine/Speed >90% pure GER ->
B1.66

25b-NBOMe Sample of 10mg
B0.94

News
- Closing the Armory
- A brand new look for Silk Road!
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes

11





Welcome, Guest. Please login or register.
Login with username, password and session length

Warning!
Only registered members are allowed to access this section.
Please login below or register an account with Playpen.

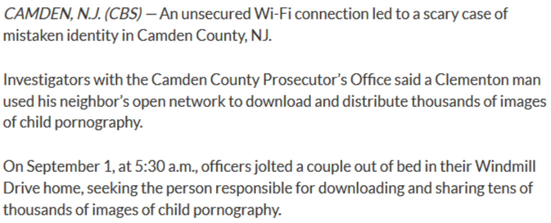
Login
Username:
Password:
Minutes to stay logged in: 60
Always stay logged in: □
Login
Forgot your password?

12

# Anti-forensic techniques

13

## Multiple internet access locations



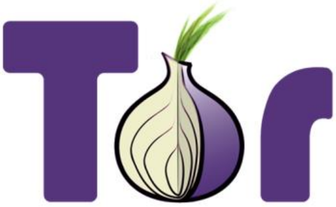
*CAMDEN, N.J. (CBS)* – An unsecured Wi-Fi connection led to a scary case of mistaken identity in Camden County, NJ.

Investigators with the Camden County Prosecutor's Office said a Clementon man used his neighbor's open network to download and distribute thousands of images of child pornography.

On September 1, at 5:30 a.m., officers jolted a couple out of bed in their Windmill Drive home, seeking the person responsible for downloading and sharing tens of thousands of images of child pornography.

14

## Anonymizing tools



15

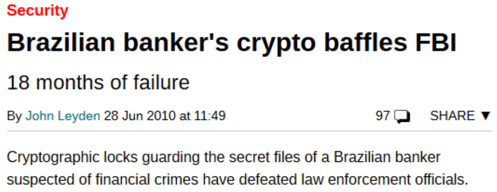
## Following the (virtual) money

- Tumbling and mixing;
- Money laundering with mining pools;
- “Reverse” loans;
- Virtual currency trading;
- In-game trading;
- The Lightning Network.

16

# Encryption, altering metadata and shredding

- Encryption, altering or erasing metadata, data shredding and attacks against forensic techniques.



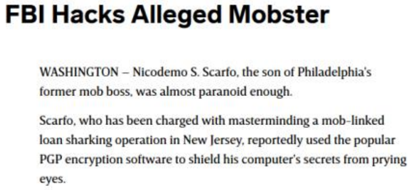
Security

**Brazilian banker's crypto baffles FBI**

18 months of failure

By John Leyden 28 Jun 2010 at 11:49 97 SHARE ▼

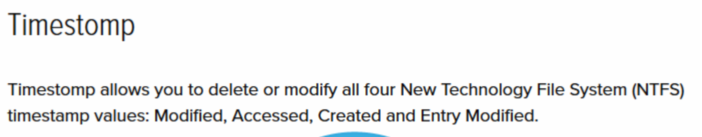
Cryptographic locks guarding the secret files of a Brazilian banker suspected of financial crimes have defeated law enforcement officials.



**FBI Hacks Alleged Mobster**

WASHINGTON – Nicodemo S. Scarfo, the son of Philadelphia's former mob boss, was almost paranoid enough.

Scarfo, who has been charged with masterminding a mob-linked loan sharking operation in New Jersey, reportedly used the popular PGP encryption software to shield his computer's secrets from prying eyes.

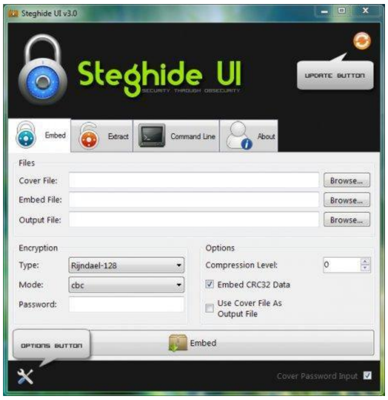


Timestomp

Timestomp allows you to delete or modify all four New Technology File System (NTFS) timestamp values: Modified, Accessed, Created and Entry Modified.

17

# Steganography



Files

Cover File:

Embed File:

Output File:

Encryption

Type: Rijndael-128

Mode: cbc

Password:

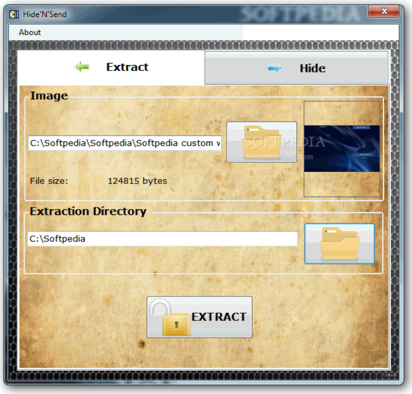
Options

Compression Level: 0

☑ Embed CRC32 Data

□ Use Cover File As Output File

Cover Password Input ☑



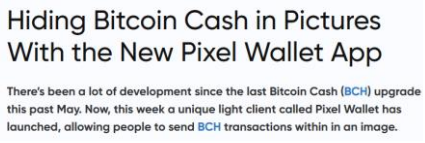
Image

C:\Softpedia\Softpedia\Softpedia custom v

File size: 124815 bytes

Extraction Directory

C:\Softpedia



Hiding Bitcoin Cash in Pictures With the New Pixel Wallet App

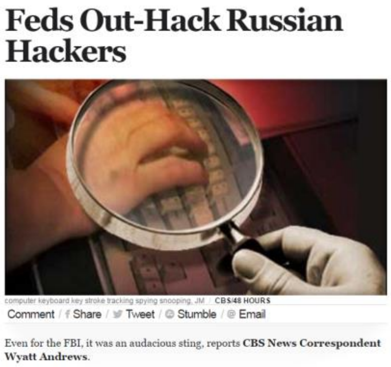
There's been a lot of development since the last Bitcoin Cash (BCH) upgrade this past May. Now, this week a unique light client called Pixel Wallet has launched, allowing people to send BCH transactions within in an image.

18

# Other difficulties in finding and collecting digital evidence

19

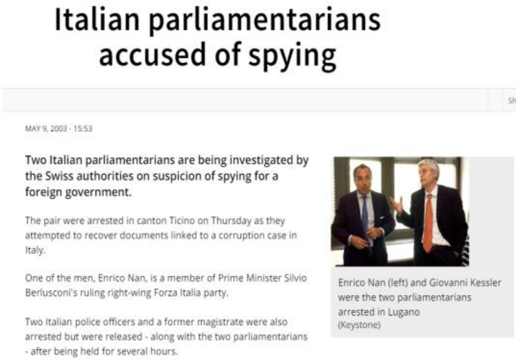
## Jurisdictional challenges



### Feds Out-Hack Russian Hackers

computer keyboard key stroke tracking spying snooping, JM / CBS/48 HOURS

Even for the FBI, it was an audacious sting, reports **CBS News Correspondent Wyatt Andrews**.



### Italian parliamentarians accused of spying

MAY 9, 2003 - 15:53

**Two Italian parliamentarians are being investigated by the Swiss authorities on suspicion of spying for a foreign government.**

The pair were arrested in canton Ticino on Thursday as they attempted to recover documents linked to a corruption case in Italy.

One of the men, Enrico Nan, is a member of Prime Minister Silvio Berlusconi's ruling right-wing Forza Italia party.

Two Italian police officers and a former magistrate were also arrested but were released - along with the two parliamentarians - after being held for several hours.

Enrico Nan (left) and Giovanni Kessler were the two parliamentarians arrested in Lugano
(Keystone)

20

# The Data Retention Directive

**The Court of Justice declares the Data Retention Directive to be invalid**

*It entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary*

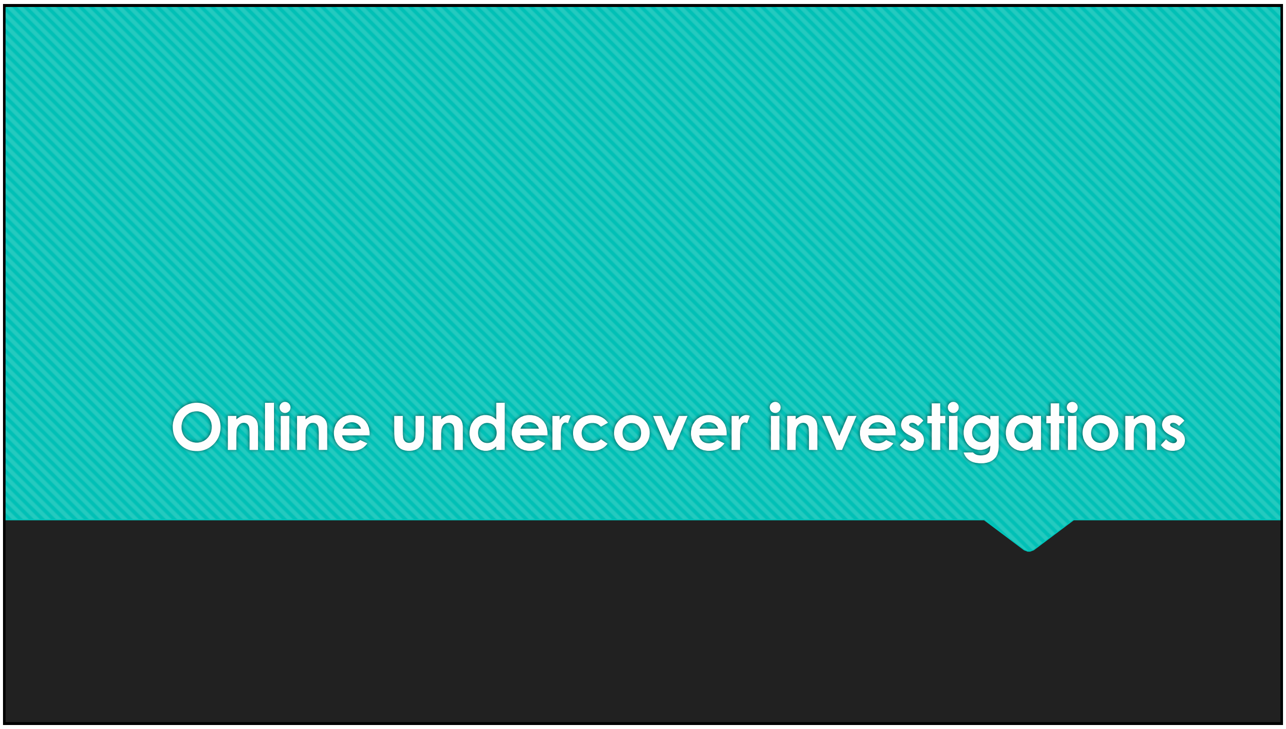
21

# Carrier-Grade NAT

Europol's Executive Director **Rob Wainwright**: *"CGN technology has created a serious online capability gap in law enforcement efforts to investigate and attribute crime. It is particularly alarming that individuals who are using mobile phones to connect to the internet to facilitate criminal activities cannot be identified because 90% of mobile internet access providers have adopted a technology which prevents them from complying with their legal obligations to identify individual subscribers. On behalf of the European law enforcement community Europol is grateful to the Estonian Presidency of the EU Council for actively exploring ways to address this urgent problem with stakeholders in the EU and industry."*

**Steven Wilson**, Head of Europol's European Cybercrime Centre, added: *"Ensuring EU law enforcement investigations are effective and result in the arrests of responsible parties is one of Europol's key functions. The issues relating to CGN, specifically the non-attribution of malicious groups and individuals, should be resolved."*

22



# Online undercover investigations

23

24

## When do we have online undercover investigations?

- Monitoring chatrooms?

> *"The risk of being overheard by an eavesdropper ... or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak"*
> – Hoffa v. United States - 385 U.S. 293, 87 S. Ct. 408 (1966)

- When does cyber-patrolling become an undercover operation?

25

## Specifics of online undercover investigations

- The beginning:
  - — Entering private/public chats;
  - — Posting comments in online content;
  - — Interacting publicly/privately with the suspect;
  - — Active/passive recording of communications.
- New forms of entrapment.

26

# Specifics of online undercover investigations

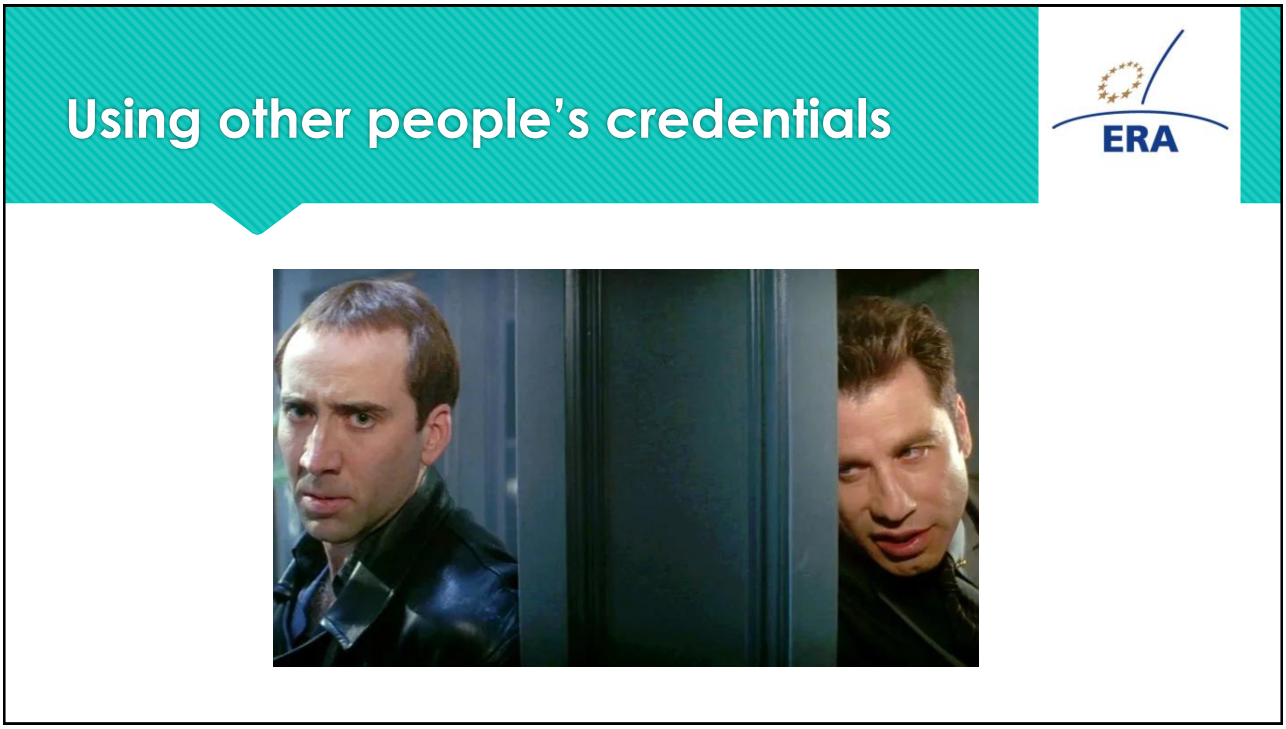
- Entrapment criteria according to ECHR (Bannikova v Russia):

  — the Court would apply the substantive test of incitement, which entailed examining
    - whether there were objective suspicions that the applicant had been involved in or was predisposed to criminal activity,
    - whether the undercover agents had merely "joined" the criminal acts or had instigated them,
    - and whether they had subjected the applicant to pressure to commit the offence

27

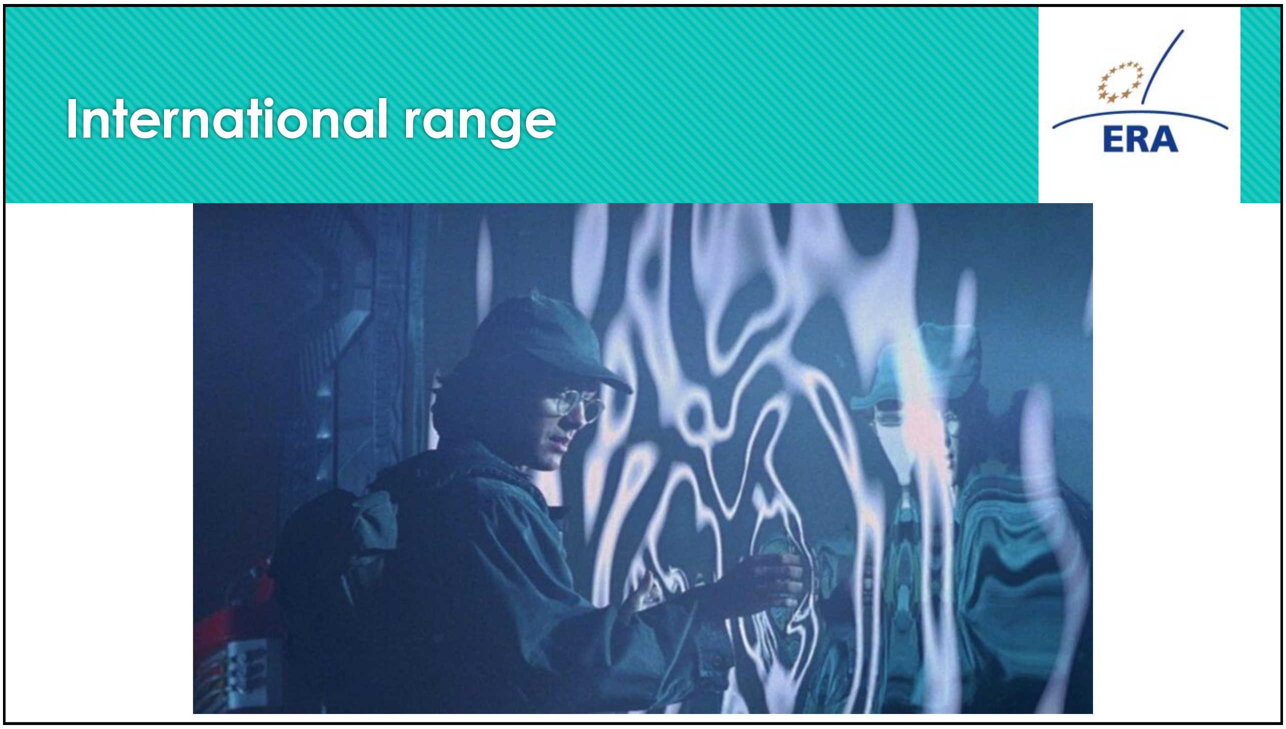
# Different personas of the undercover agent

28



## Using other people's credentials

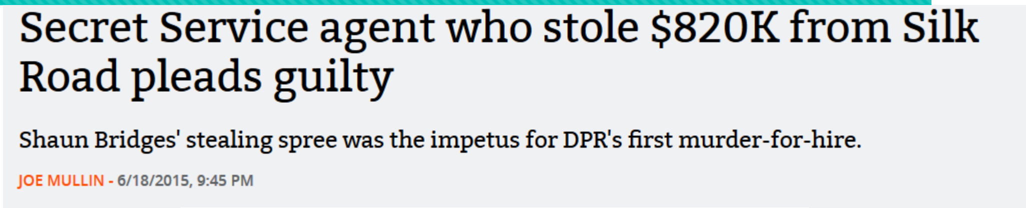
29



## International range

30

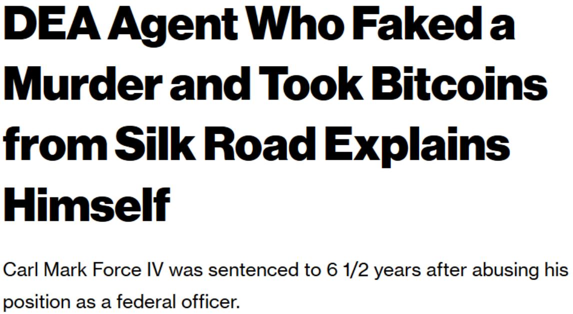
## Risks



Secret Service agent who stole $820K from Silk Road pleads guilty

Shaun Bridges' stealing spree was the impetus for DPR's first murder-for-hire.

JOE MULLIN - 6/18/2015, 9:45 PM



**DEA Agent Who Faked a Murder and Took Bitcoins from Silk Road Explains Himself**

Carl Mark Force IV was sentenced to 6 1/2 years after abusing his position as a federal officer.

31

## The need for a legal framework

- Judicial warrant specifying (law or good practices):
  - Need for the operation (proportionality assessment)
  - Duration and purposes of the operation;
  - List of usable nicknames;
  - List of computer systems or locations from which the operation may take place;
  - List of actions that are authorized (e.g. recording of communications)
  - In case the undercover agent is not from law enforcement, limitation of access to the credentials.

32

## The need for a legal framework

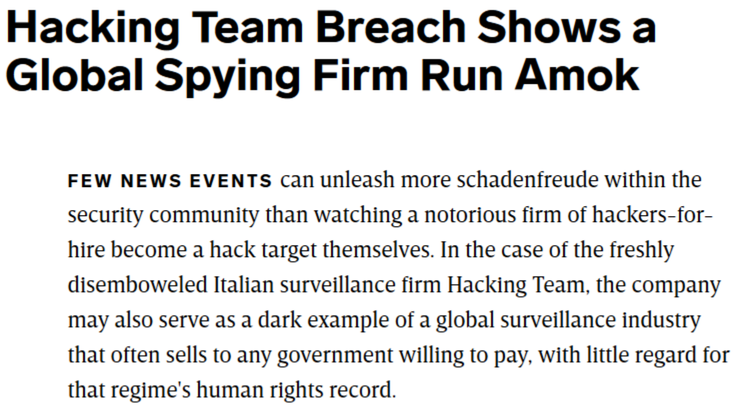
- Clarification of the criteria for the existence of an online undercover operation;
- Obligation to disclose the existence of an undercover operation with adequate reporting of the undercover agent's actions;
- Allowing the undercover agent to send illegal content when strictly necessary;
- Allowing for the monitorization of these files as they are resent;
- Restricting cases where infiltration is made with existing accounts;
- Adapting the crimes subject to this measure to cybercrime.

33

## The use of malware and legal hacking to collect evidence

34

## Use of malware and legal hacking



### Hacking Team Breach Shows a Global Spying Firm Run Amok

**FEW NEWS EVENTS** can unleash more schadenfreude within the security community than watching a notorious firm of hackers-for-hire become a hack target themselves. In the case of the freshly disemboweled Italian surveillance firm Hacking Team, the company may also serve as a dark example of a global surveillance industry that often sells to any government willing to pay, with little regard for that regime's human rights record.

35

## Use of malware and legal hacking

- The RCS Galileo
  - — Interception of communications;
  - — Remote activation of webcams and microphones
  - — Activation of GPS;
  - — Keylogger instalation:
  - — Recording of communications through IM (including Skype)
  - — Screenshots of the user’s activity.

36

## Minimum legal requirements

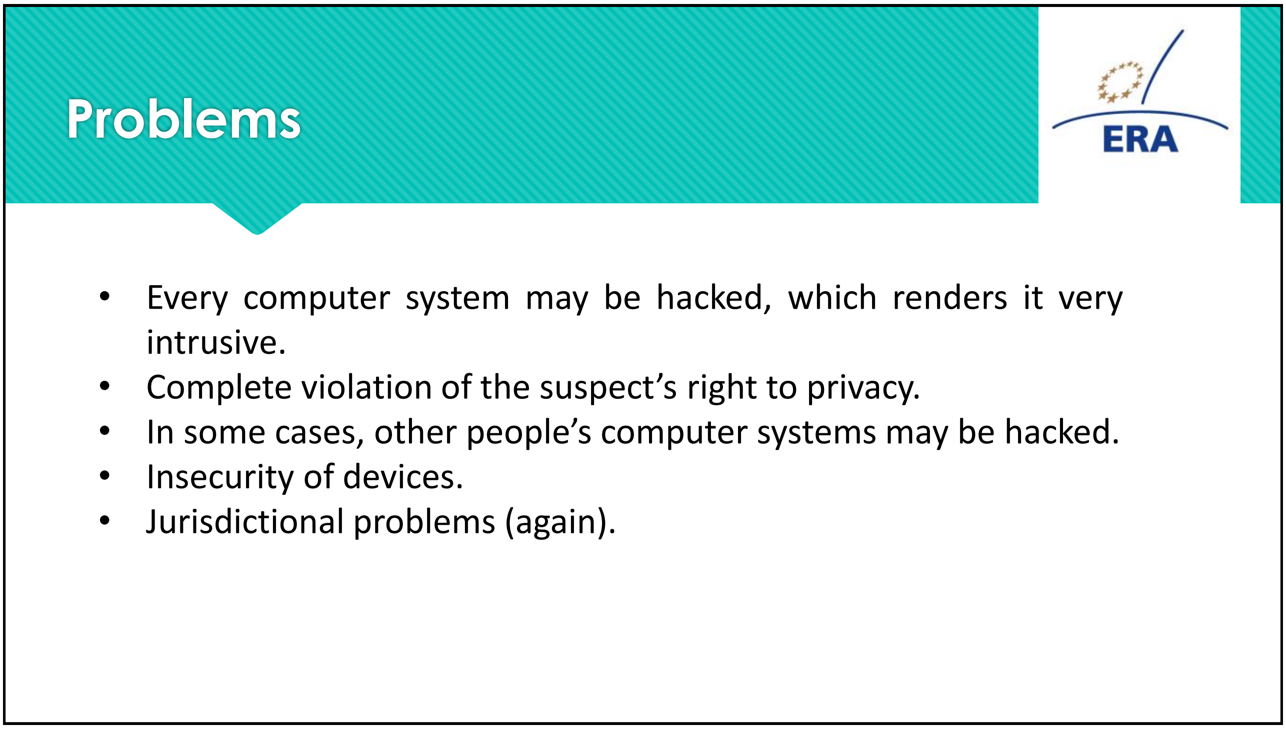
ERA

- A clear distinction between the so-called online searches and the use of equipment to monitor its surroundings;
- Restricted only to the most serious offences;
- Judicial warrant stating clearly:
  - — Target devices and the content sought;
  - — Scope of the measure (suspects, duration, data);
  - — The terms in which the data may be searched and accessed;
  - — Persons authorized to use it in a given investigation;
  - — Authorization to keep copies of the information.

## Minimum legal requirements

ERA

- The need for periodic review of the need for this measure;
- Implementation of a certification system for the *malware*;
- Right of the defence to access all of the relevant information, excluding that which is strictly operational;
- Creation of measures for uninstalling the malware.
- The right of the defence to confirm that the malware used is certified.



## Problems

- Every computer system may be hacked, which renders it very intrusive.
- Complete violation of the suspect’s right to privacy.
- In some cases, other people’s computer systems may be hacked.
- Insecurity of devices.
- Jurisdictional problems (again).

39

## Legal safeguards, reliability and the right of defence

40

# Reporting

ERA

«***The case-specific notes maintained by digital investigators for each evidential item they work with should document what processes were performed*** *(e.g., recovery of deleted files and keyword searches), what the overall results were of each process, and any significant findings. In this way, digital investigators can reduce the risk of forgetting to run certain processes on a particular evidential item.* ***In addition, this documentation can help with peer review and external evaluation of results, enabling someone else to repeat any of the steps that were performed and independently locate and verify important findings***» - EOGHAN CASEY, «Applying Forensic Science to Computers», *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Dir. EOGHAN CASEY), 3.ª ed. USA: Elsevier, 2011, p. 473.

41

# Disclosure

ERA

- A copy of every computer system or data has to be disclosed to the defense as soon as possible;
- Disclosure needs to be in an easily readable and useable format;
- Non-disclosure has to be exceptional and subject to appropriate reasoning;
- If the defendant is in pre-trial detention, conditions should be made available for him to participate in the defense.
- Computer systems and evidence that has not been used in the indictment should be returned to the defendant, unless other legal ground for retaining it exists;
- Whenever a copy is denied to the defense, it should be done based on the opinion of an independent expert.

42

## Broadness of searches

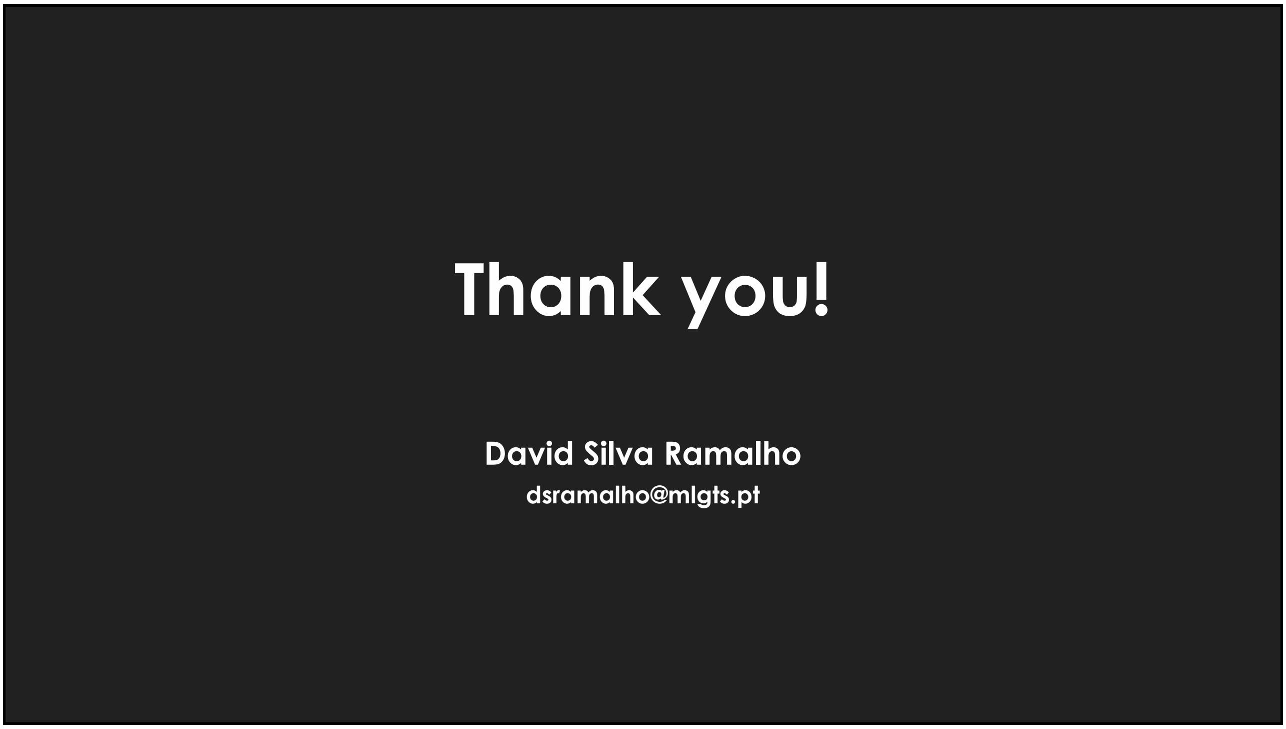
- Computer warrants need to be sufficiently narrow so as to avoid fishing expeditions.
- It is frequent that the investigator uses excessively broad terms and ends up finding evidence of different offences.
- Either search terms are previously defined in the warrant or casual findings must be made irrelevant.
- Incentive for broad searches needs to be reduced.
- This may happen by limiting the relevant evidence as the one found on the basis of a previously defined investigation method.

43

## Computer literacy

- During the investigation phase, an experienced and trained Prosecutor should be in charge.
- Courts need to learn or to seek to be informed by an independent party of the subject at stake and the specificities of digital evidence;
- The presumption of infallibility of digital evidence needs to be challenged. So does the presumption that being tech-savy = being a cybercriminal or that bitcoin = money laundering.
- The violation of digital forensics procedures has to be seen as ground for exclusion of evidence;
- Physical word’s experience is seldom inapplicable to cybercrime.

44



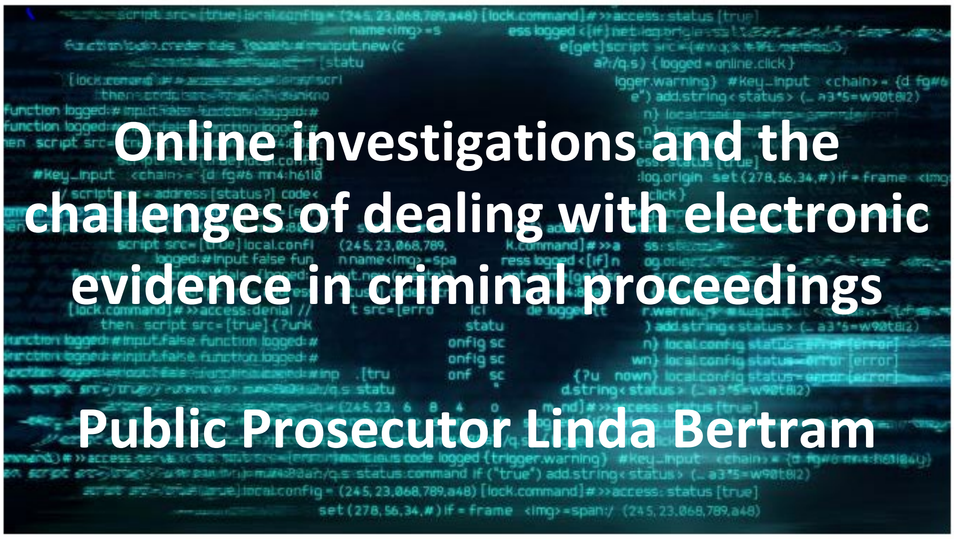
# Thank you!

**David Silva Ramalho**

**dsramalho@mlgts.pt**

45

# OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES FOCUS ON THE WHOLE LIFE CYCLE OF E-EVIDENCE (CUSTODY CHAIN, PRESENTATION & ASSESSMENT) ERA - Cracow, 24-25 March 2022



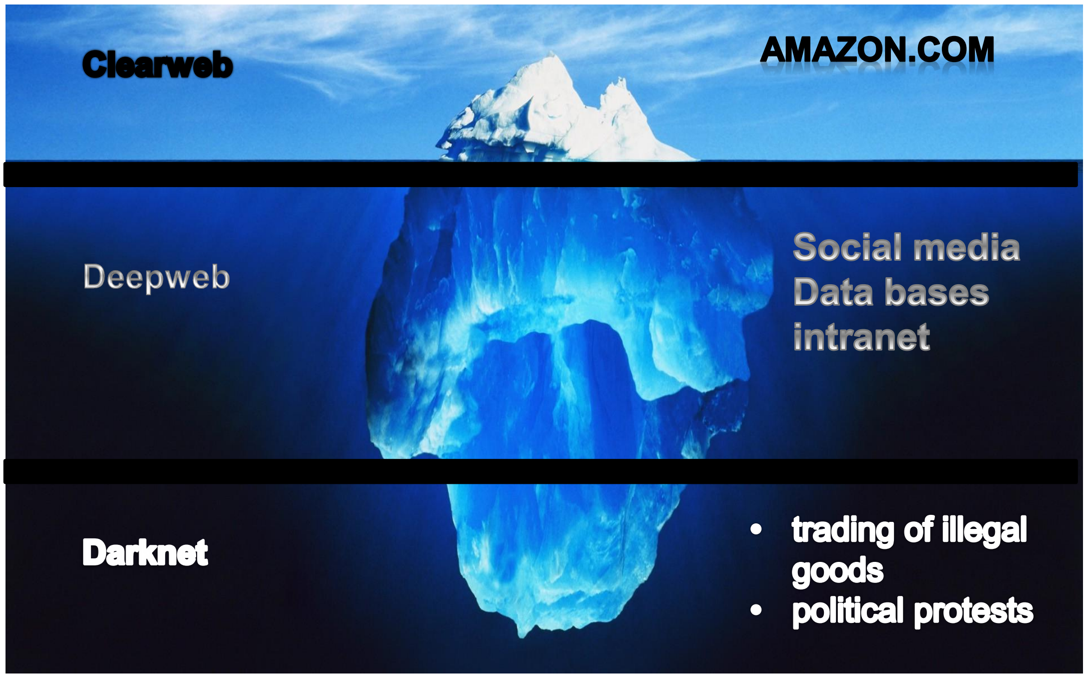
## Online investigations and the challenges of dealing with electronic evidence in criminal proceedings

Public Prosecutor Linda Bertram

Foto: James Thew / Fotolia

## Cybercrime – what are we talking about?

## Darknet, DeepWeb, Clearweb???



## Measures depend upon the electronic environment …

„Classical“ measures:

- IP-tracking
- wire-tapping
- images
- payment information
- OSINT

…most likely won‘t work in the darknet…

- identify TOR entry guard
- undercover investigations

# Almost always you‘ll need help from abroad

## International Mutual Assistance in Criminal Matters

- preservation request
- freezing order
- EIO
- MLAT

Soon to be:

- e-Evidence regulation
- CLOUD act

# Help with and coordination of international cooperation on the judicial side

EUROJUST

Steering EIOs and MLATs to the competent authority via the desks as well as

coordination of conferences for the development of common strategies and the exchange of information between representatives of law enforcement agencies and judicial authorities from the participating countries and consulting with agreeing upon a handling code according to the Europol standard

## 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.

## 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.

## 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.

## Expert Witness

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

## 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

## 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!

Quelle:Sophos

## The beginning of our investigation

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

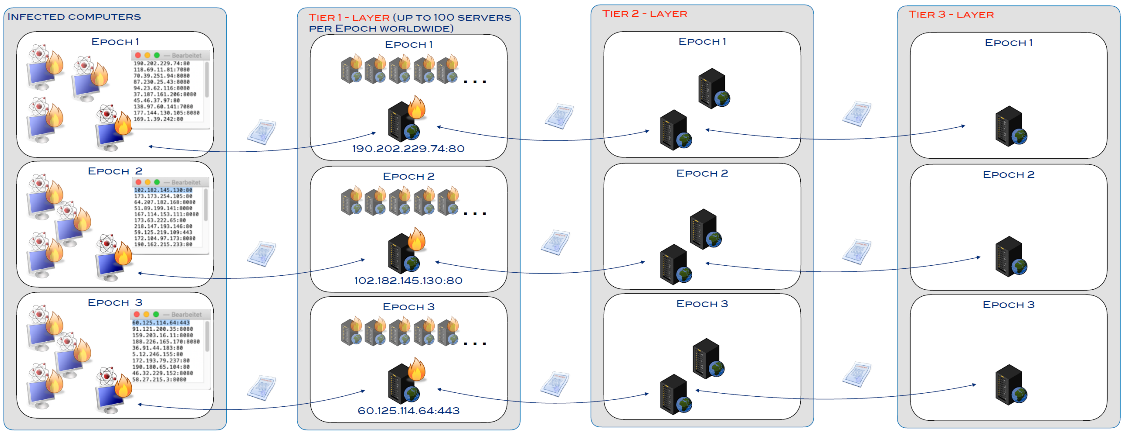
## The beginning of our investigation

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

# Who has been affected in Germany?

- courts
- federal agencies
- municipalities
- university hospitals
- medical practices
- universities
- schools
- companies

# EMOTET infrastructure in general

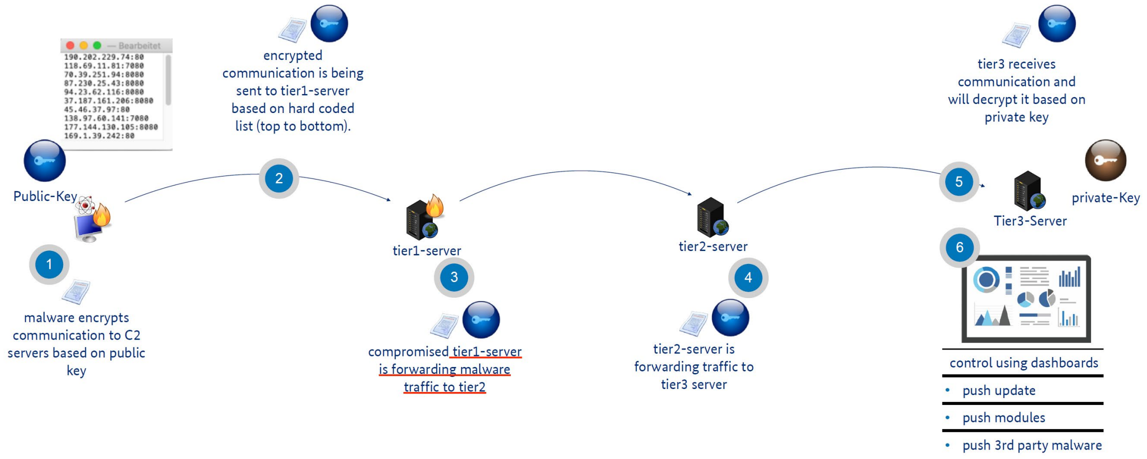


```
190.202.229.74:80
118.69.11.81:7080
70.39.251.94:8080
87.230.25.43:8080
94.23.62.116:8080
37.187.161.206:8080
45.46.37.97:80
138.97.60.141:7080
177.144.130.105:8080
169.1.39.242:80
```

```
102.182.145.130:80
173.173.254.105:80
64.207.182.168:8080
51.89.199.141:8080
167.114.153.111:8080
173.63.222.65:80
218.147.193.146:80
59.125.219.109:443
172.104.97.173:8080
190.162.215.233:80
```

```
60.125.114.64:443
91.121.200.35:8080
159.203.16.11:8080
188.226.165.170:8080
36.91.44.183:80
5.12.246.155:80
172.193.79.237:80
190.180.65.104:80
46.32.229.152:8080
58.27.215.3:8080
```

# EMOTET infrastructure in general



```
— Bearbeitet
190.202.229.74:80
118.69.11.81:7080
70.39.251.94:8080
87.230.25.43:8080
94.23.62.116:8080
37.187.161.206:8080
45.46.37.97:80
138.97.60.141:7080
177.144.130.105:8080
169.1.39.242:80
```

Public-Key

1 malware encrypts communication to C2 servers based on public key

2 encrypted communication is being sent to tier1-server based on hard coded list (top to bottom).

tier1-server

3 compromised tier1-server is forwarding malware traffic to tier2

tier2-server

4 tier2-server is forwarding traffic to tier3 server

5 tier3 receives communication and will decrypt it based on private key

Tier3-Server

private-Key

6 control using dashboards

- push update
- push modules
- push 3rd party malware

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

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

## Coordination of international cooperation

EUROJUST

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

EUROPOL

## Challenges and solutions

- Planning of an international action day with joint actions in individual countries, including national measures as well as measures by way of mutual legal assistance under COVID-19 restrictions
  - ➢ operational centers at Europol and Eurojust with colleagues on site as well as supporting video conferences
  - ➢ national operational centers

## Challenges and solutions

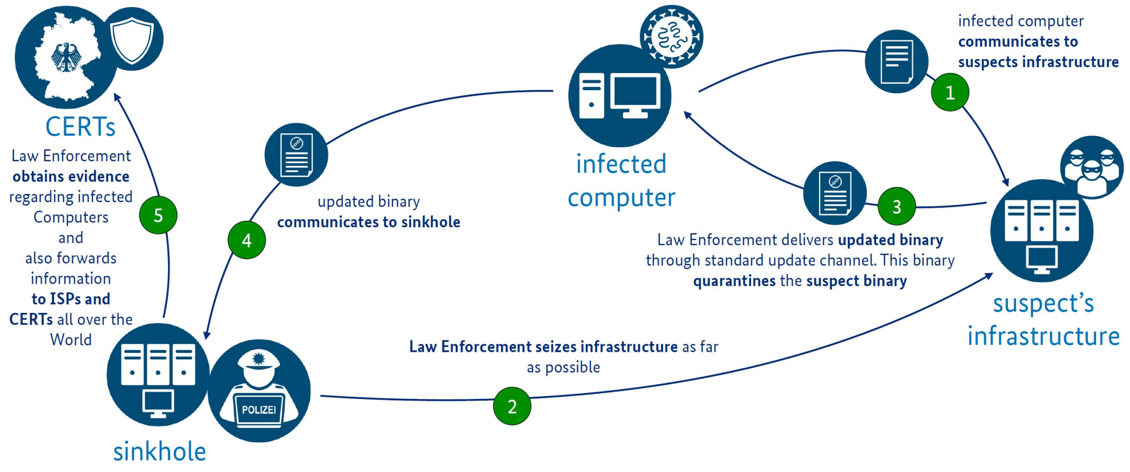
- Legal basis of rerouting the traffic of the purely IP-based, constantly changing Emotet infrastructure
  - ➢ „ hybrid court order" with elements of seizure, as well as the usage of the so-called annex competence with extension to systems newly discovered through technical measures

## Challenges and solutions

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

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

## Challenges and solutions



infected computer

1 infected computer **communicates to suspects infrastructure**

suspect's infrastructure

2 **Law Enforcement seizes infrastructure** as far as possible

3 Law Enforcement delivers **updated binary** through standard update channel. This binary **quarantines** the **suspect binary**

4 updated binary **communicates to sinkhole**

sinkhole

5 CERTs

Law Enforcement **obtains evidence** regarding infected Computers and also forwards information **to ISPs and CERTs** all over the World

# State of play

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

# Thank you very much!
# Questions?

Linda Bertram

Staatsanwältin/
Public Prosecutor

Generalstaatsanwaltschaft Frankfurt am Main
- Zentralstelle zur Bekämpfung der Internetkriminalität- /
Prosecutor General's Office
– Cyber Crime Center –

**I**nternational **L**egal **A**ssistance

Konrad-Adenauer-Straße 15
60313 Frankfurt am Main

Phone: + 49 611 3265 8718 **Mob.: + 49 171 28 93 504 (SPOC for ILA 24/7)**

Fax: + 49 611 3265 8704 Mail: linda.bertram@gsta.justiz.hessen.de

# Cross-border access to data and jurisdictional issues

## Draft e-evidence package: European Production Orders

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

**Dr. Maša Galič**
**Assistant professor of privacy and criminal procedure law**
**Vrije Universiteit Amsterdam (VU University Amsterdam)**

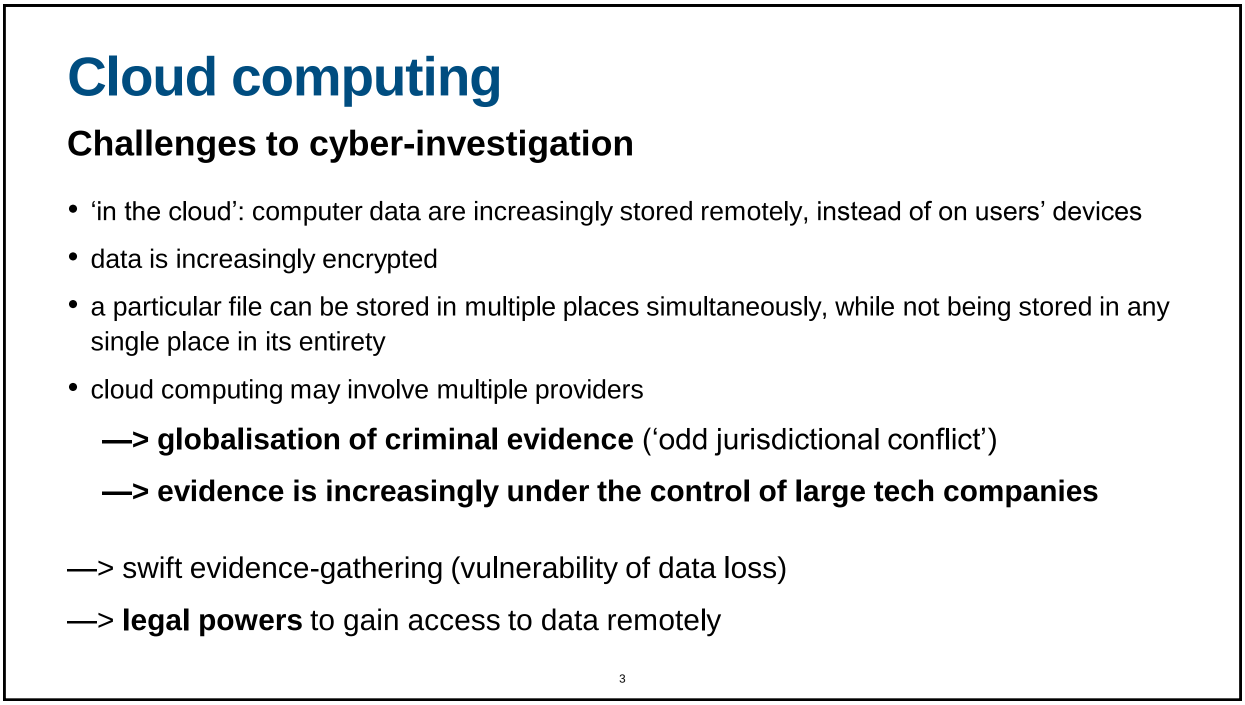
VU VRIJE UNIVERSITEIT AMSTERDAM

1

## Structure

1. **Introduction**
   - cloud computing + challenges to cyber-investigation
   - existing cross-border evidence-gathering powers + issues
2. **Recent legal developments concerning cross-border evidence-gathering**
3. **Draft e-evidence package**
4. **European Production Order (EPO)**
   - scope: service provider + new categorisation of data
   - conditions for issuing an EPO
   - transmission of the EPO + enforcement procedure
   - notification obligation + fundamental rights protection

2



# Cloud computing

## Challenges to cyber-investigation

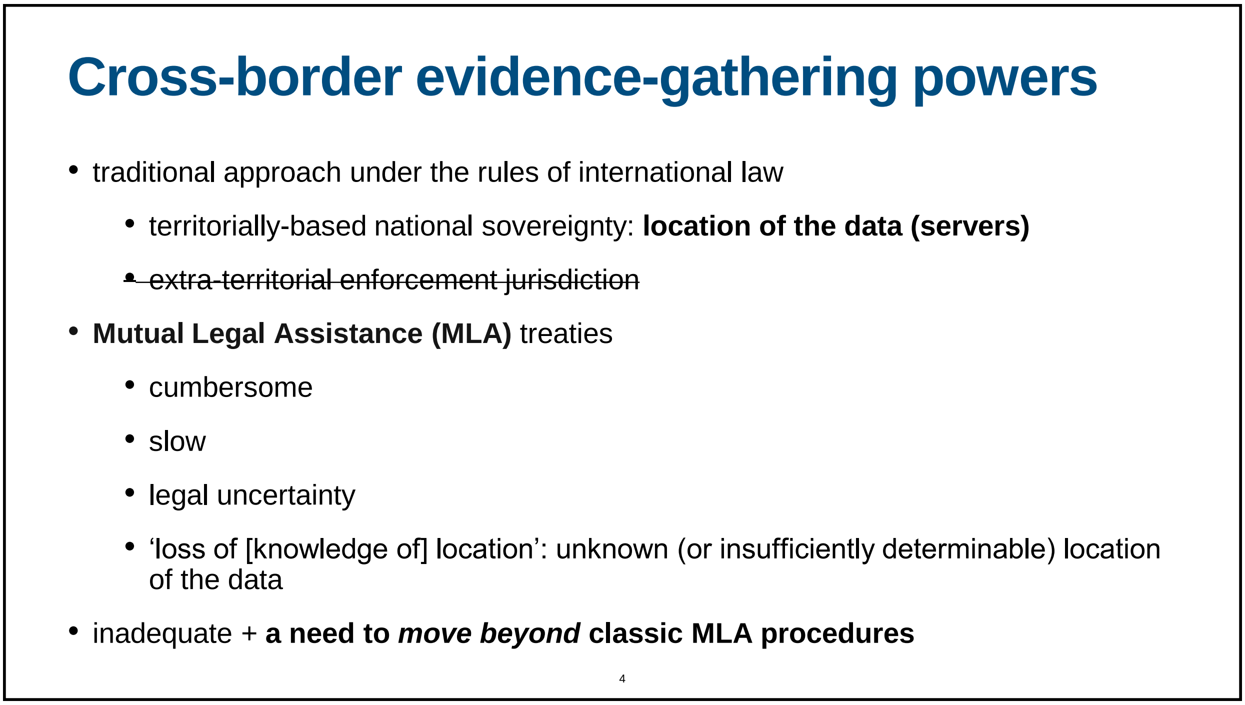
- ‘in the cloud’: computer data are increasingly stored remotely, instead of on users’ devices
- data is increasingly encrypted
- a particular file can be stored in multiple places simultaneously, while not being stored in any single place in its entirety
- cloud computing may involve multiple providers

**—> globalisation of criminal evidence** (‘odd jurisdictional conflict’)

**—> evidence is increasingly under the control of large tech companies**

—> swift evidence-gathering (vulnerability of data loss)

—> **legal powers** to gain access to data remotely



# Cross-border evidence-gathering powers

- traditional approach under the rules of international law
  - territorially-based national sovereignty: **location of the data (servers)**
  - ~~extra-territorial enforcement jurisdiction~~
- **Mutual Legal Assistance (MLA)** treaties
  - cumbersome
  - slow
  - legal uncertainty
  - ‘loss of [knowledge of] location’: unknown (or insufficiently determinable) location of the data
- inadequate + **a need to *move beyond* classic MLA procedures**

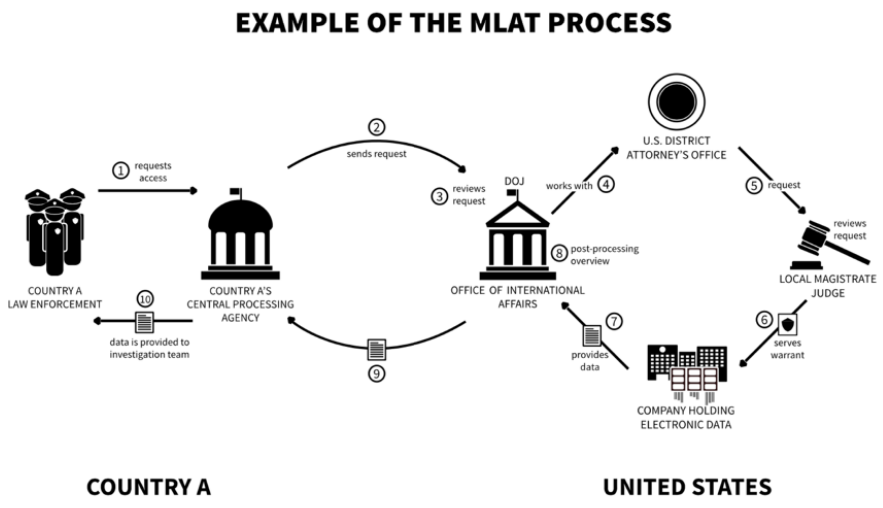

EXAMPLE OF THE MLAT PROCESS
1 requests access
2 sends request
3 reviews request
DOJ
works with 4
U.S. DISTRICT ATTORNEY'S OFFICE
5 request
reviews request
LOCAL MAGISTRATE JUDGE
8 post-processing overview
COUNTRY A LAW ENFORCEMENT
COUNTRY A'S CENTRAL PROCESSING AGENCY
OFFICE OF INTERNATIONAL AFFAIRS
10
data is provided to investigation team
9
7
provides data
6
serves warrant
COMPANY HOLDING ELECTRONIC DATA
COUNTRY A
UNITED STATES

*Diagram 1 Example of the U.S. Mutual Legal Assistance Treaty Process for Electronic Evidence*

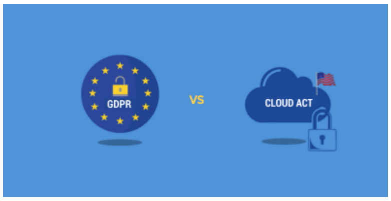
Lin & Fidler, Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement (2017, p. 3)

5

- voluntary cooperation by service providers
- unilateral approach
- invasive forms of cross-border access to data

6

- a fragmented framework
- conflicting legal obligations

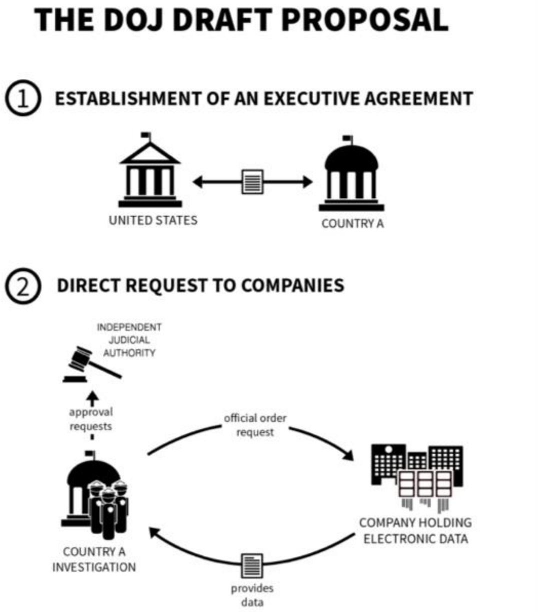


- legal uncertainty
- weakened human rights protection + other safeguards (e.g., double criminality)

## Many recent developments

**New laws and legal proposals**

- European Investigation Order Directive (2014)
- CLOUD Act (2018)
  - executive agreement between US and UK (2019)
  - executive agreement between US and Australia (2021)
  - formal negotiations of such an agreement between US and EU (2019-)
- Second Additional Protocol to the Cybercrime Convention (2021)
- **draft E-evidence legislative package (Regulation + Directive): ‘European CLOUD Act’**



## THE DOJ DRAFT PROPOSAL

1. ESTABLISHMENT OF AN EXECUTIVE AGREEMENT

UNITED STATES

COUNTRY A

2. DIRECT REQUEST TO COMPANIES

INDEPENDENT JUDICIAL AUTHORITY

approval requests

official order request

COMPANY HOLDING ELECTRONIC DATA

provides data

COUNTRY A INVESTIGATION

*Diagram 2 Diagram of DOJ Cross-Border Data Access Proposal*

Lin & Fidler (2017), p. 6

# Draft e-evidence package

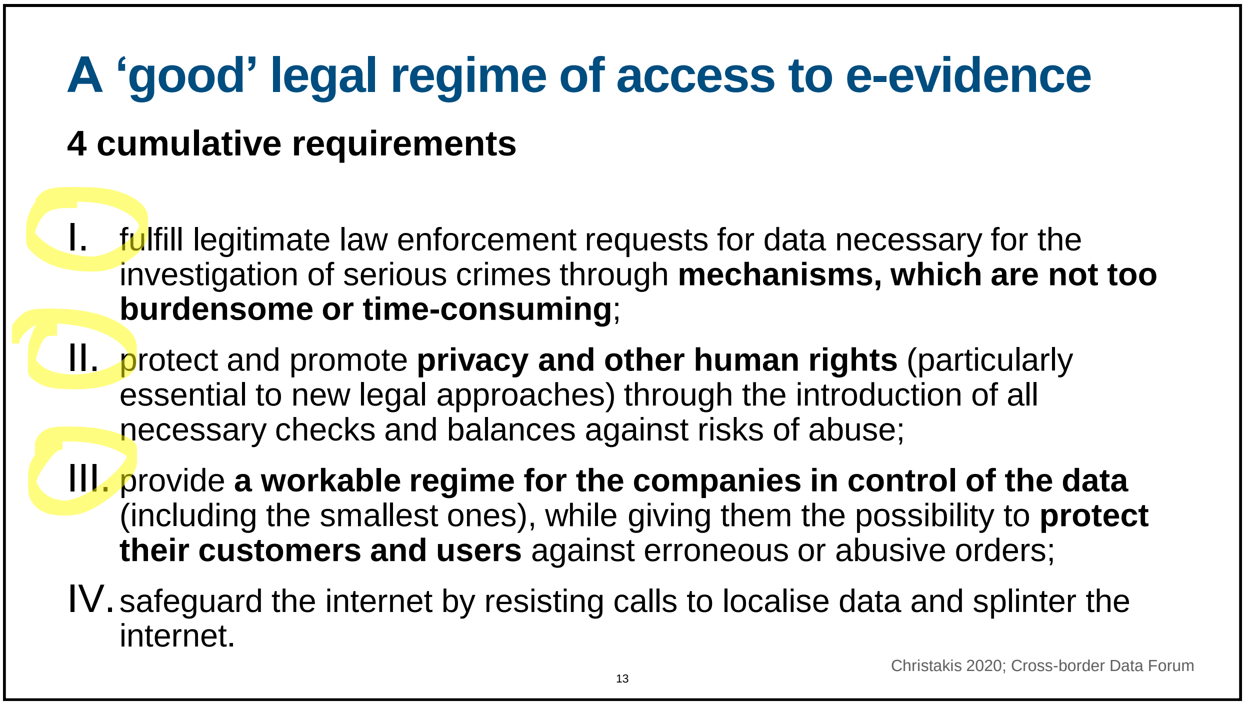
# Draft E-evidence package

## The need to access data in the hands of service providers abroad

- **goal**: to develop a common framework for cooperation with service providers (established or represented in another MS) for the purpose of obtaining specific categories of data and to improve legal certainty and clarity
- **regardless of the location where the data are stored**
  - **Regulation**: '**direct cooperation**' (~~unmediated access~~) between a public authority of a MS ('issuing authority') and a service provider in another MS
    - **European Production Order**
    - European Preservation Order
  - **Directive**: obliging services providers '**offering services in the EU**' to designate a legal representative for the purpose of receiving and responding to orders requesting data ('knowing whom to contact when seeking disclosure of data')

# 3 versions of the Regulation

- Commission: 'original proposal' (Apr 2018)
- Council: 'general approach' (Dec 2018)
- Parliament: 'human rights-centred' (Dec 2020)



# A ‘good’ legal regime of access to e-evidence

**4 cumulative requirements**

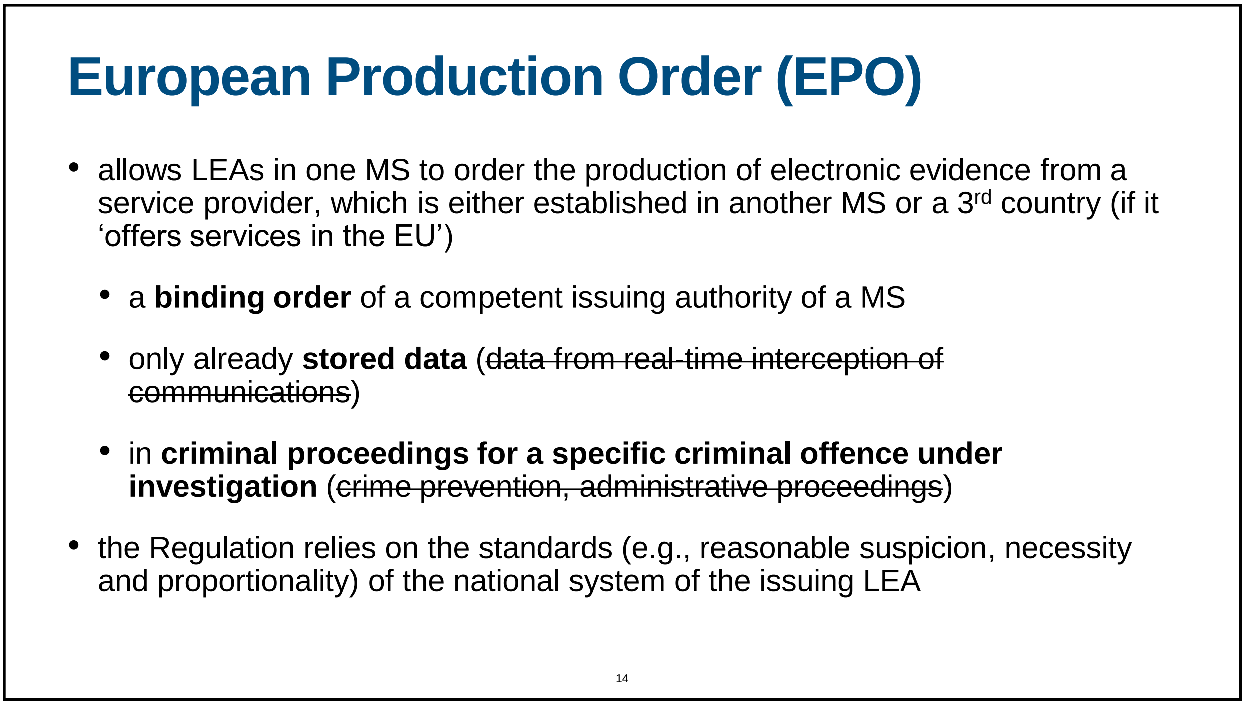
I. fulfill legitimate law enforcement requests for data necessary for the investigation of serious crimes through **mechanisms, which are not too burdensome or time-consuming**;

II. protect and promote **privacy and other human rights** (particularly essential to new legal approaches) through the introduction of all necessary checks and balances against risks of abuse;

III. provide **a workable regime for the companies in control of the data** (including the smallest ones), while giving them the possibility to **protect their customers and users** against erroneous or abusive orders;

IV. safeguard the internet by resisting calls to localise data and splinter the internet.

Christakis 2020; Cross-border Data Forum



# European Production Order (EPO)

- allows LEAs in one MS to order the production of electronic evidence from a service provider, which is either established in another MS or a 3rd country (if it ‘offers services in the EU’)
  - a **binding order** of a competent issuing authority of a MS
  - only already **stored data** (~~data from real-time interception of communications~~)
  - in **criminal proceedings for a specific criminal offence under investigation** (~~crime prevention, administrative proceedings~~)
- the Regulation relies on the standards (e.g., reasonable suspicion, necessity and proportionality) of the national system of the issuing LEA

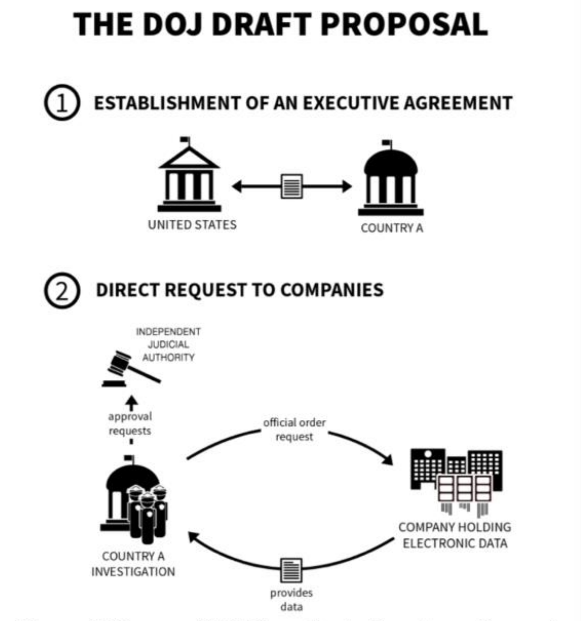

THE DOJ DRAFT PROPOSAL
1 ESTABLISHMENT OF AN EXECUTIVE AGREEMENT
UNITED STATES
COUNTRY A
2 DIRECT REQUEST TO COMPANIES
INDEPENDENT JUDICIAL AUTHORITY
approval requests
official order request
COMPANY HOLDING ELECTRONIC DATA
COUNTRY A INVESTIGATION
provides data

*Diagram 2 Diagram of DOJ Cross-Border Data Access Proposal*

Lin & Fidler (2017), p. 6

# Service provider

- a natural or legal person providing
  - **electronic communication services**: internet access service, interpersonal communications service and services consisting wholly or mainly in the conveyance of signals

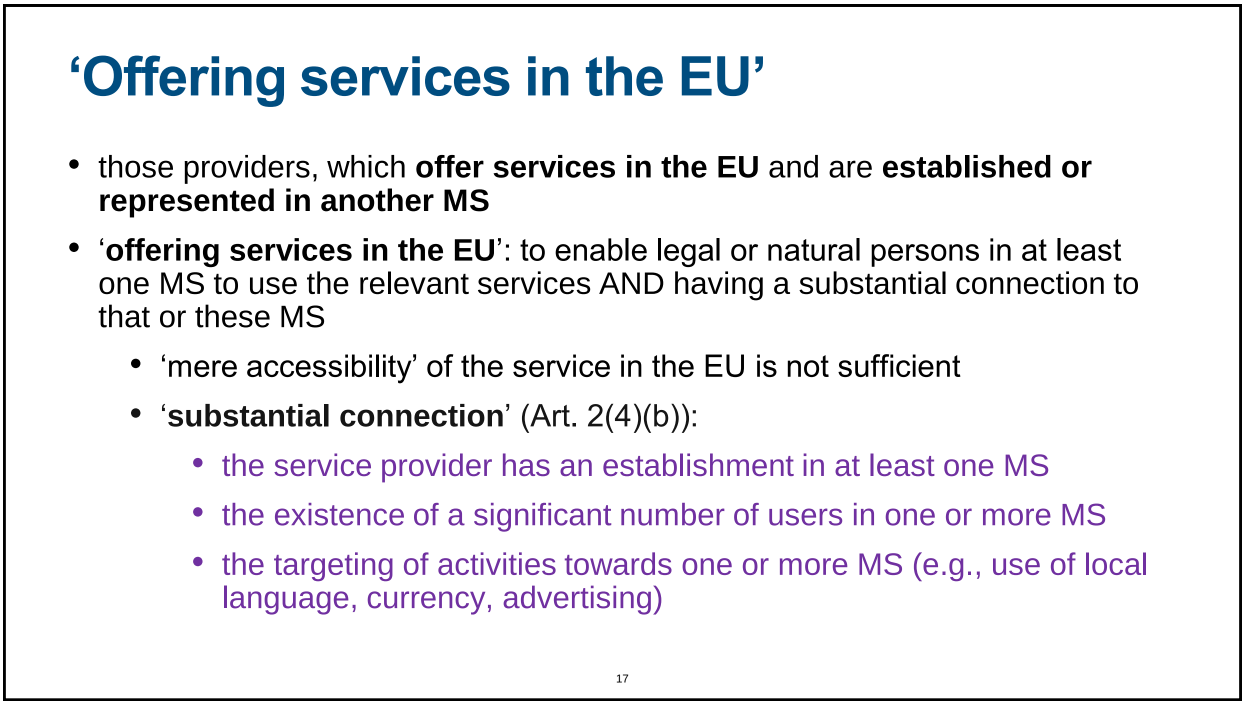
    —> e.g., traditional telecommunications services (voice telephony, SMS, internet access service), voice over IP (Skype) , instant messaging (WhatsApp) and web-based email services (**'over-the-top communication services' – OTTs**)

  - **information society-services** for which the storage of data is a defining component of the service

    —> e.g., social networks (Facebook, Twitter), online marketplaces (eBay, Amazon marketplace), cloud-based services (Microsoft, Dropbox, Amazon Web Services), other hosting service providers (Bluehost)

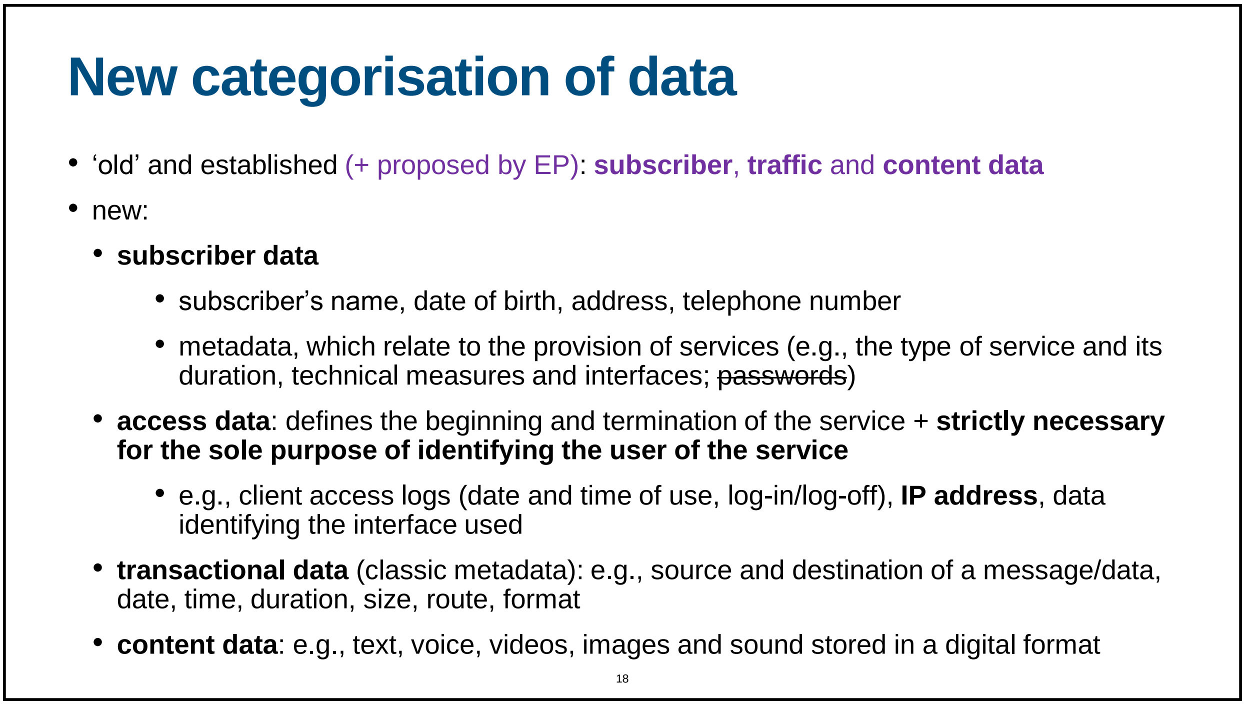
  - **internet domain name and IP numbering services**

    —> IP address providers, domain name registries, domain name registrars (GoDaddy), proxy services



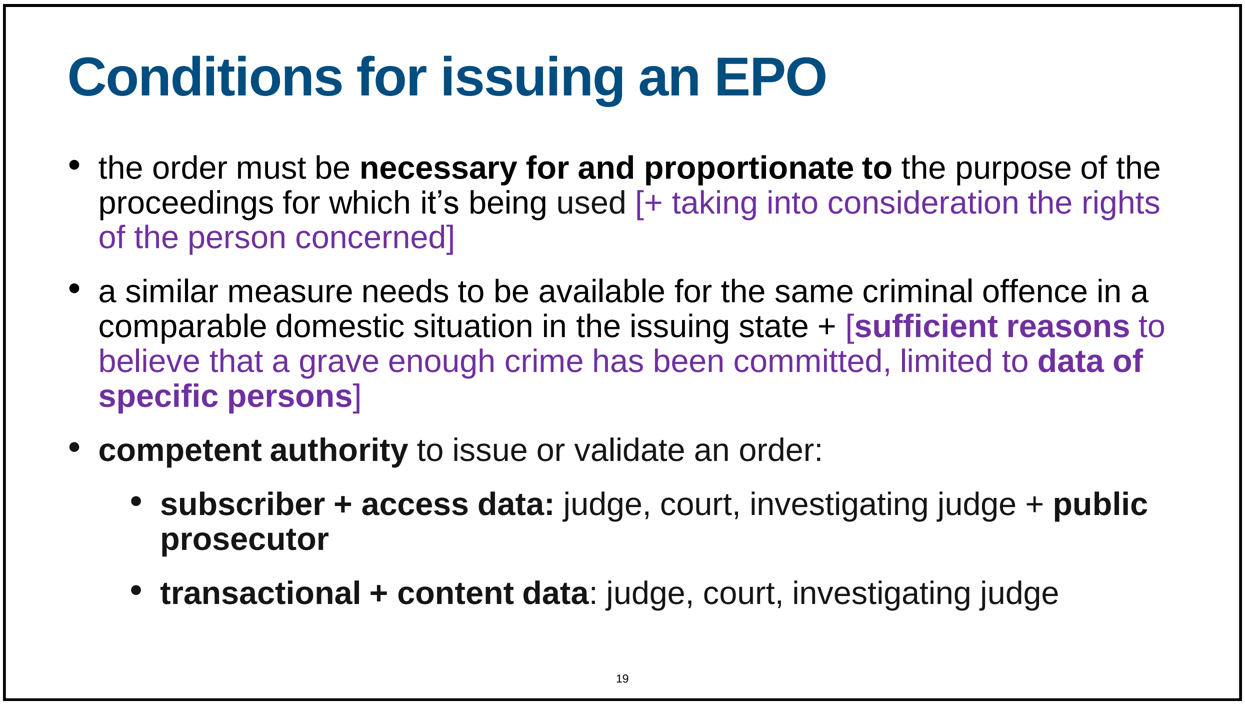
# ‘Offering services in the EU’

- those providers, which **offer services in the EU** and are **established or represented in another MS**
- ‘**offering services in the EU**’: to enable legal or natural persons in at least one MS to use the relevant services AND having a substantial connection to that or these MS
  - ‘mere accessibility’ of the service in the EU is not sufficient
  - ‘**substantial connection**’ (Art. 2(4)(b)):
    - the service provider has an establishment in at least one MS
    - the existence of a significant number of users in one or more MS
    - the targeting of activities towards one or more MS (e.g., use of local language, currency, advertising)



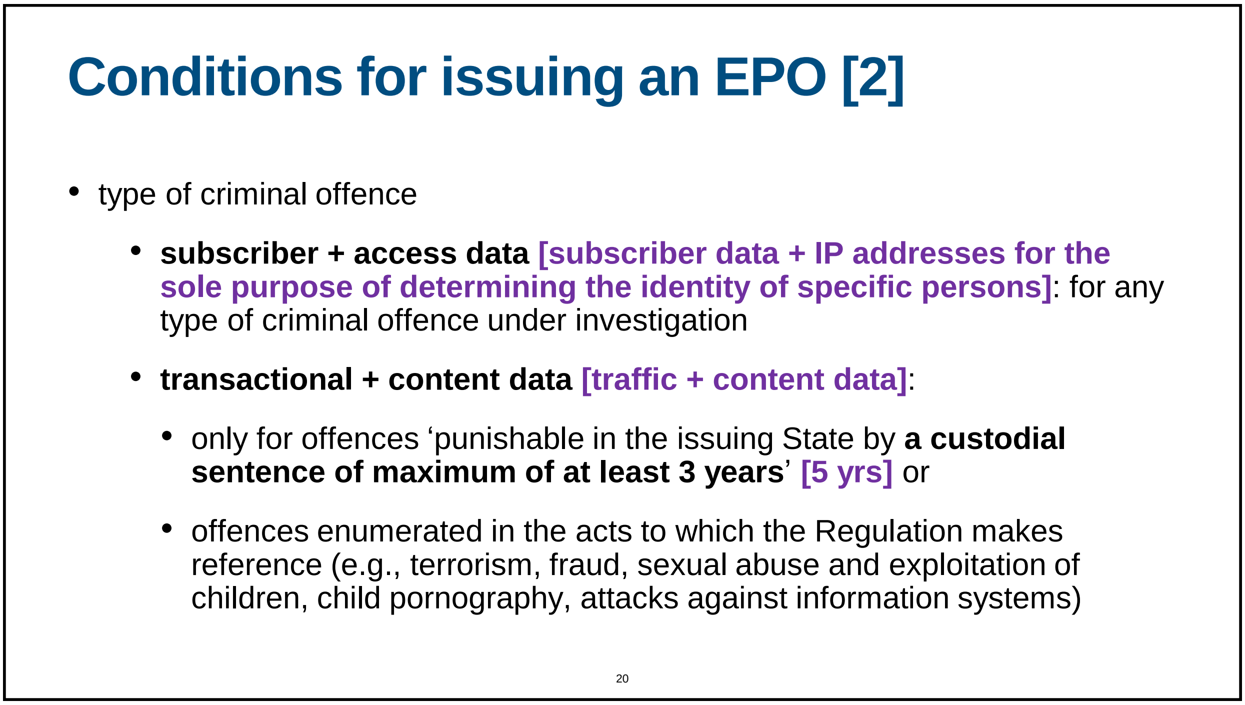
# New categorisation of data

- ‘old’ and established (+ proposed by EP): **subscriber**, **traffic** and **content data**
- new:
  - **subscriber data**
    - subscriber’s name, date of birth, address, telephone number
    - metadata, which relate to the provision of services (e.g., the type of service and its duration, technical measures and interfaces; ~~passwords~~)
  - **access data**: defines the beginning and termination of the service + **strictly necessary for the sole purpose of identifying the user of the service**
    - e.g., client access logs (date and time of use, log-in/log-off), **IP address**, data identifying the interface used
  - **transactional data** (classic metadata): e.g., source and destination of a message/data, date, time, duration, size, route, format
  - **content data**: e.g., text, voice, videos, images and sound stored in a digital format



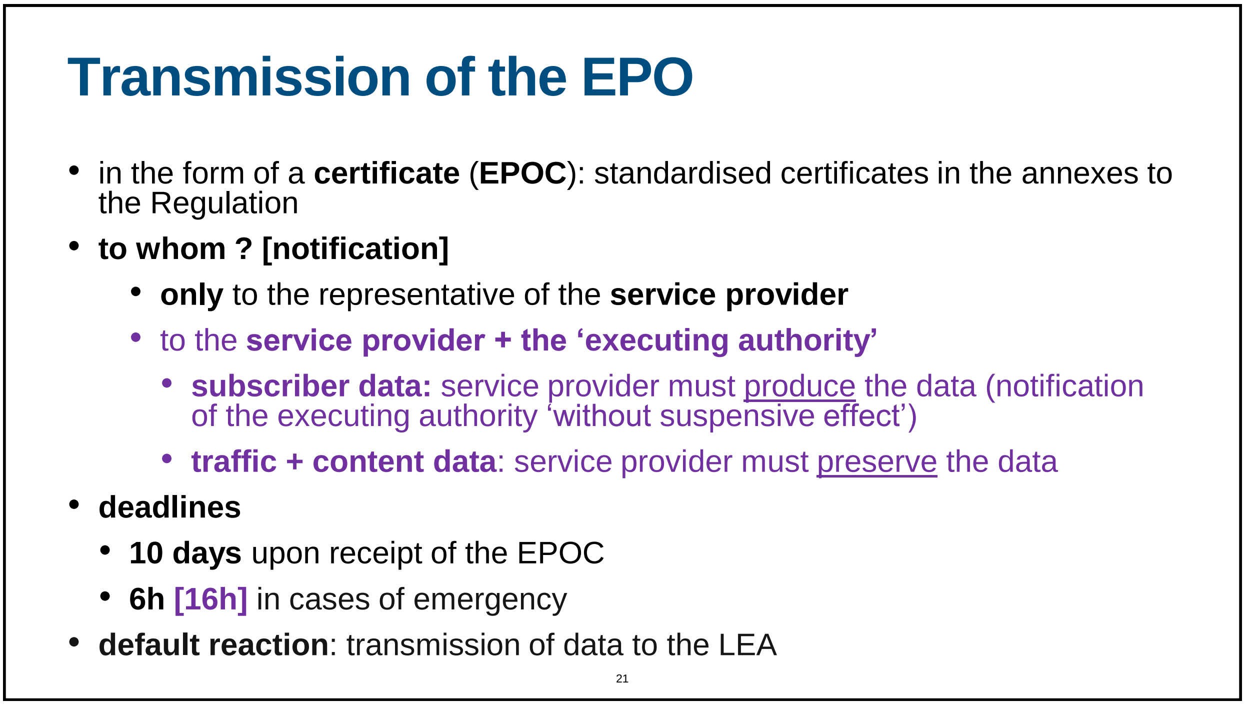
# Conditions for issuing an EPO

- the order must be **necessary for and proportionate to** the purpose of the proceedings for which it’s being used [+ taking into consideration the rights of the person concerned]
- a similar measure needs to be available for the same criminal offence in a comparable domestic situation in the issuing state + [**sufficient reasons** to believe that a grave enough crime has been committed, limited to **data of specific persons**]
- **competent authority** to issue or validate an order:
  - **subscriber + access data:** judge, court, investigating judge + **public prosecutor**
  - **transactional + content data**: judge, court, investigating judge



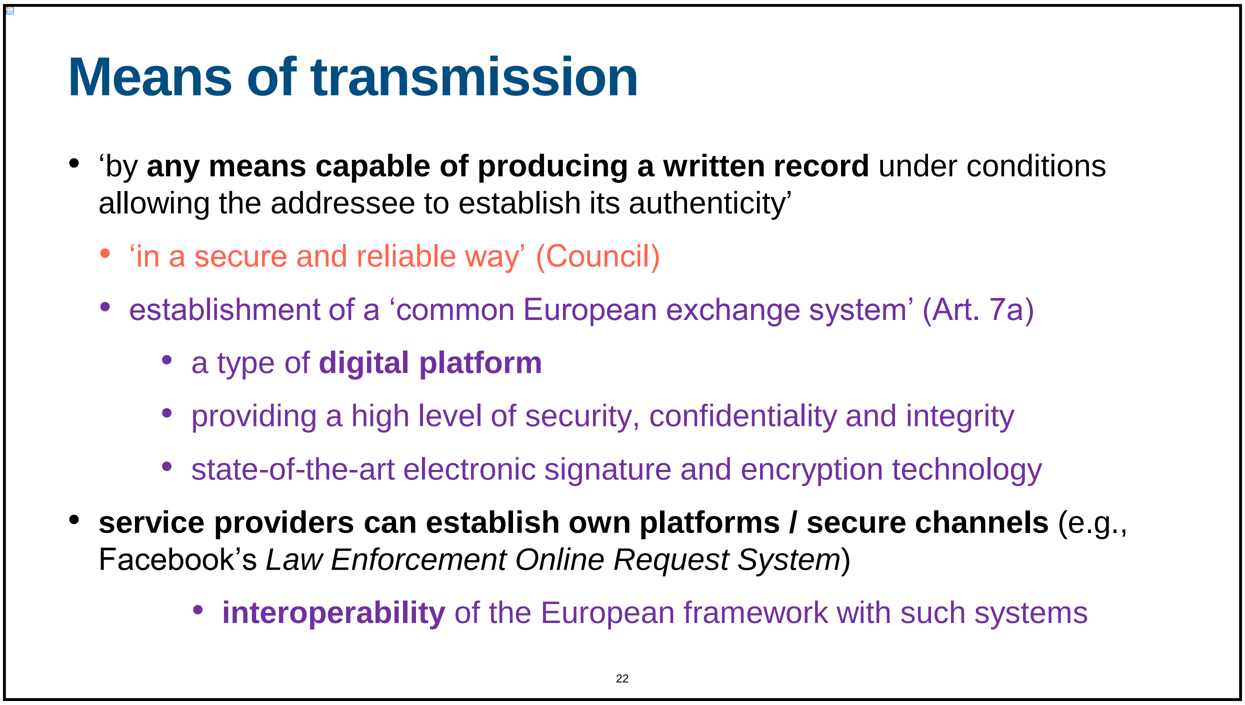
# Conditions for issuing an EPO [2]

- type of criminal offence
  - **subscriber + access data [subscriber data + IP addresses for the sole purpose of determining the identity of specific persons]**: for any type of criminal offence under investigation
  - **transactional + content data [traffic + content data]**:
    - only for offences ‘punishable in the issuing State by **a custodial sentence of maximum of at least 3 years**’ **[5 yrs]** or
    - offences enumerated in the acts to which the Regulation makes reference (e.g., terrorism, fraud, sexual abuse and exploitation of children, child pornography, attacks against information systems)



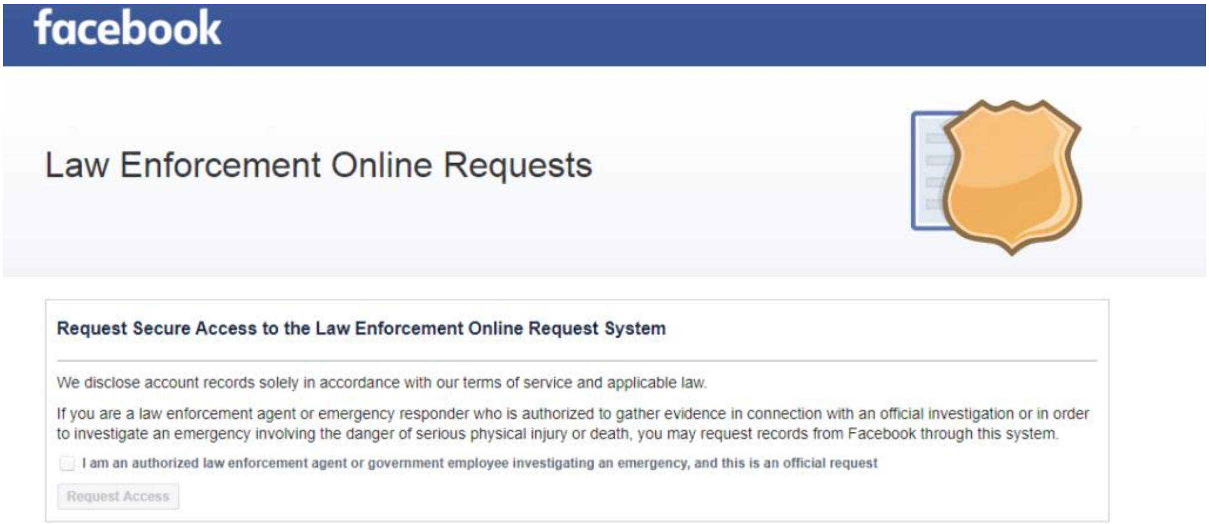
# Transmission of the EPO

- in the form of a **certificate** (**EPOC**): standardised certificates in the annexes to the Regulation
- **to whom ? [notification]**
  - **only** to the representative of the **service provider**
  - to the **service provider + the 'executing authority'**
    - **subscriber data:** service provider must produce the data (notification of the executing authority 'without suspensive effect')
    - **traffic + content data**: service provider must preserve the data
- **deadlines**
  - **10 days** upon receipt of the EPOC
  - **6h** **[16h]** in cases of emergency
- **default reaction**: transmission of data to the LEA



# Means of transmission

- 'by **any means capable of producing a written record** under conditions allowing the addressee to establish its authenticity'
  - 'in a secure and reliable way' (Council)
  - establishment of a 'common European exchange system' (Art. 7a)
    - a type of **digital platform**
    - providing a high level of security, confidentiality and integrity
    - state-of-the-art electronic signature and encryption technology
- **service providers can establish own platforms / secure channels** (e.g., Facebook's *Law Enforcement Online Request System*)
  - **interoperability** of the European framework with such systems



Law Enforcement Online Requests

**Request Secure Access to the Law Enforcement Online Request System**

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

□ I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

Source: https://www.facebook.com/records

# Enforcement procedure: EC [± Council]

**Service provider** may ‘**refuse to comply**’ with the order in the event that:

1. the order is incomplete, contains manifest errors or insufficient information for execution

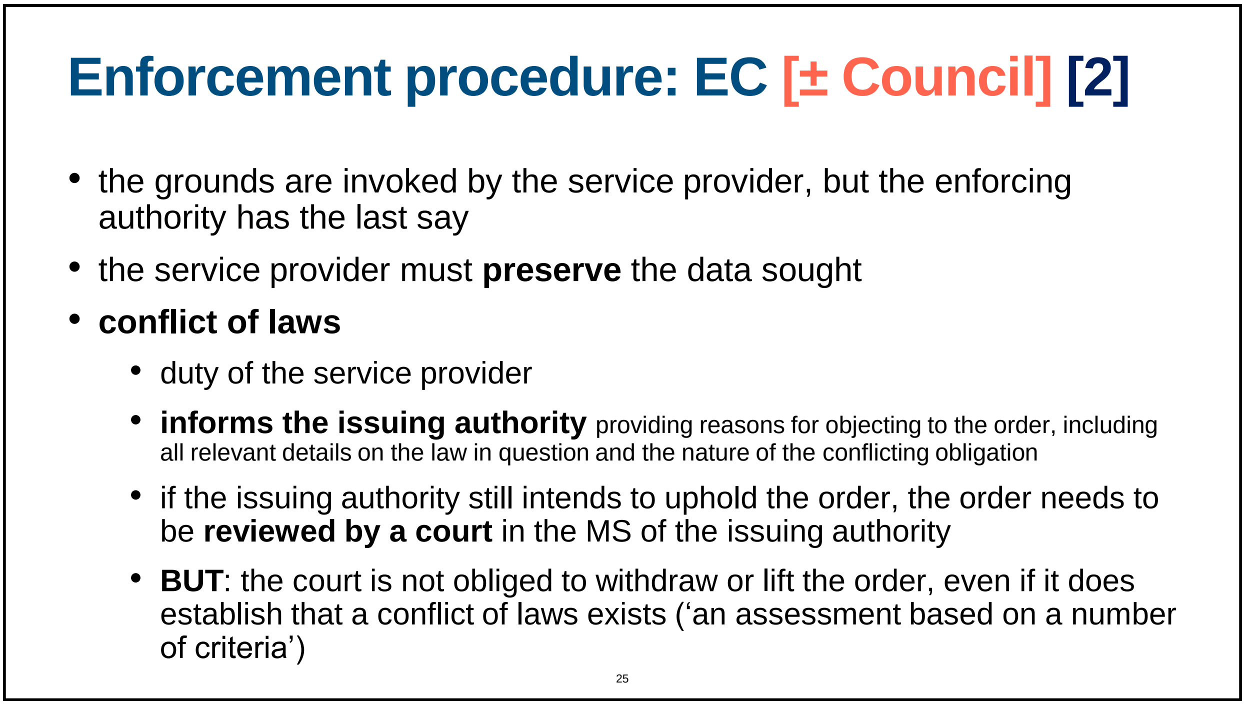
   **--> inform the issuing authority** and ask the issuing authority for **clarification**

2. *force majeure*, *de facto* impossibility, not a customer, data deleted

   **--> inform the issuing authority**

3. the order manifestly violates the CFREU or is manifestly abusive **[deleted by the Council]**

   **--> inform the issuing authority + notify the competent authority of the enforcing state** (which ‘may’ seek clarifications from the issuing authority)

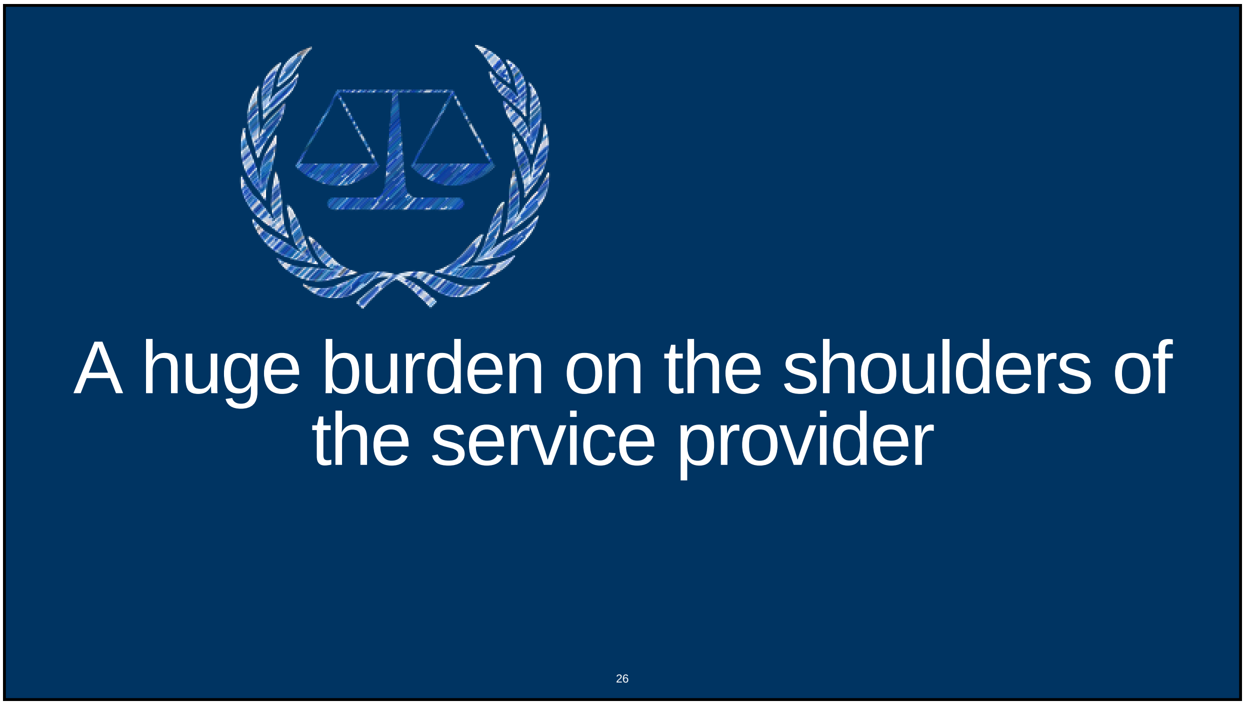


## Enforcement procedure: EC [± Council] [2]

- the grounds are invoked by the service provider, but the enforcing authority has the last say
- the service provider must **preserve** the data sought
- **conflict of laws**
  - duty of the service provider
  - **informs the issuing authority** providing reasons for objecting to the order, including all relevant details on the law in question and the nature of the conflicting obligation
  - if the issuing authority still intends to uphold the order, the order needs to be **reviewed by a court** in the MS of the issuing authority
  - **BUT**: the court is not obliged to withdraw or lift the order, even if it does establish that a conflict of laws exists (‘an assessment based on a number of criteria’)

25

25



A huge burden on the shoulders of the service provider

26

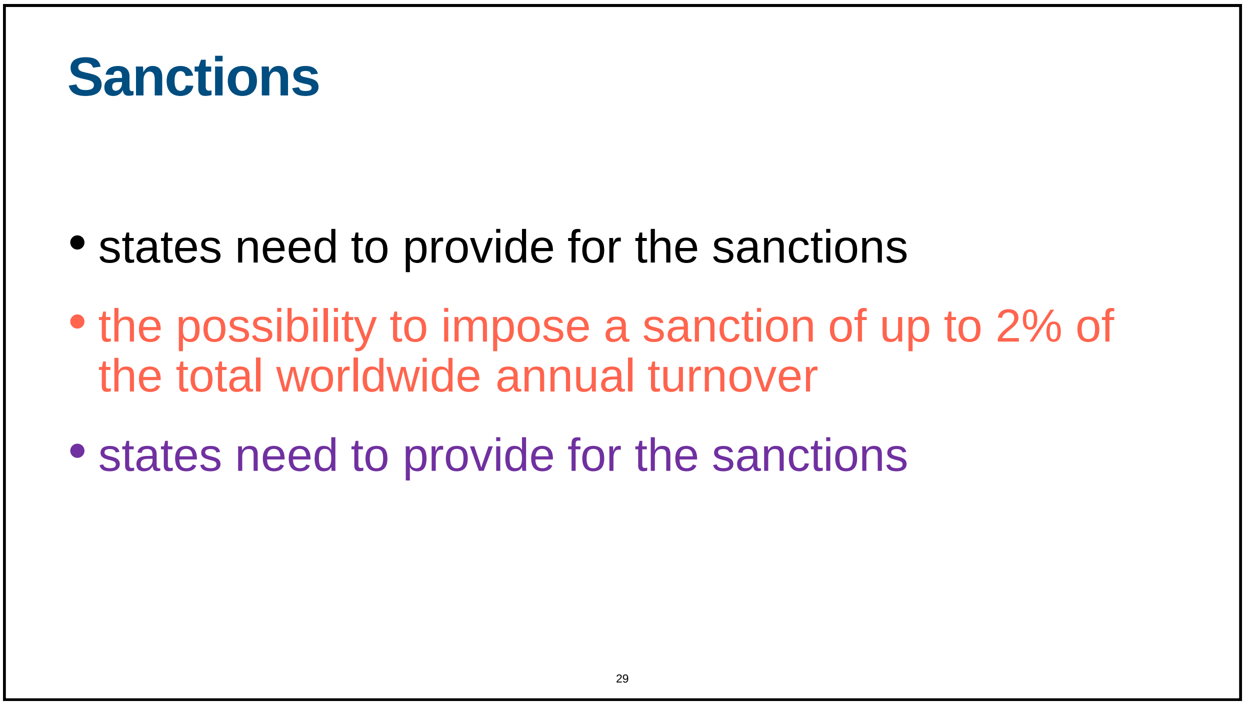
26

# Enforcement procedure: EP

- transmission of the EPO both to **the service provider + the enforcing (executing) authority**
- **grounds for refusal of enforcement**
  - conditions for issuing EPO are not fulfilled (e.g., competent authority, type of crime)
  - contrary to *ne bis in idem*
  - incompatible with MS's obligations stemming from Art. 6 TEU
  - immunity, privilege, limitation of criminal liability, freedom of press/expression under the law of the executing state

  → additional grounds for refusal for **traffic + content data**:
  - essential national security and similar interests
  - double criminality
  - conflict of laws
- obligatory **consultation** with the issuing authority before refusal to enforce is taken

# Burden on the shoulders of the executing authority

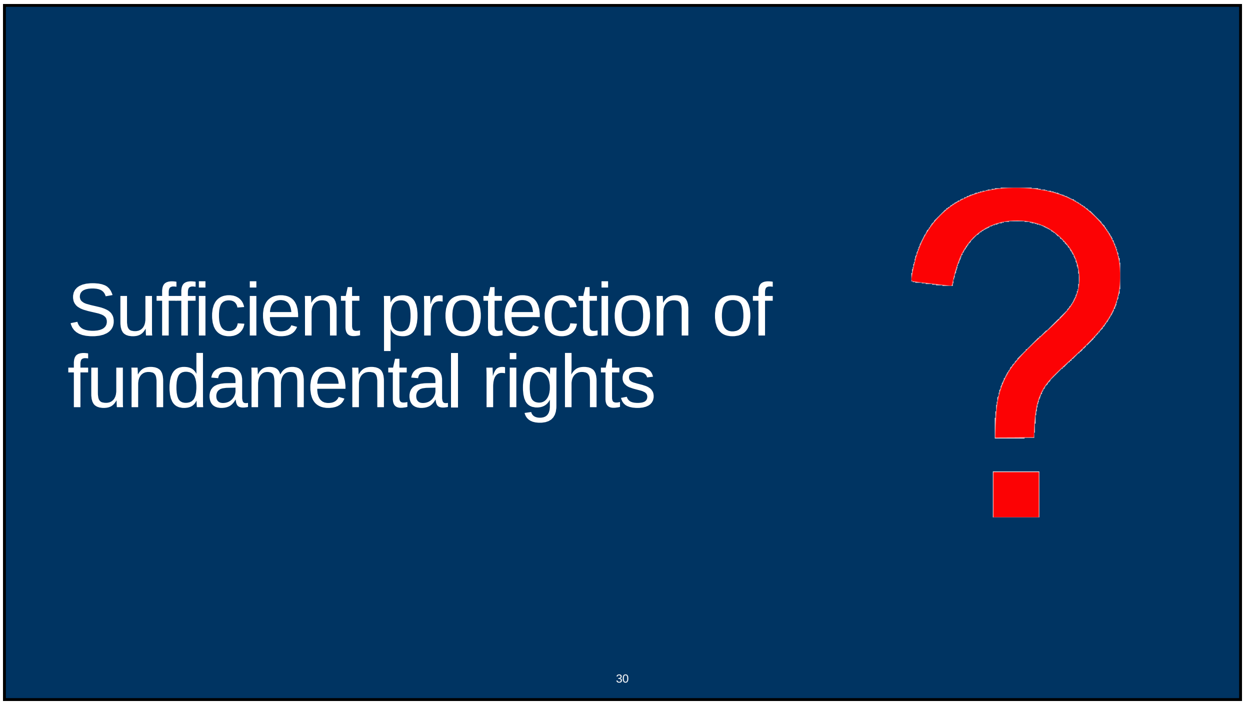


## Sanctions

- states need to provide for the sanctions
- the possibility to impose a sanction of up to 2% of the total worldwide annual turnover
- states need to provide for the sanctions

29

29



# Sufficient protection of fundamental rights

?

30

30

# A general fundamental rights clause

**Art. 1(2) Regulation**

This Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in [the Charter and] Article 6 of the TEU, including the rights of defence of persons subject to criminal proceedings, and any obligations incumbent on law enforcement or judicial authorities [or service providers] in this respect shall remain unaffected.

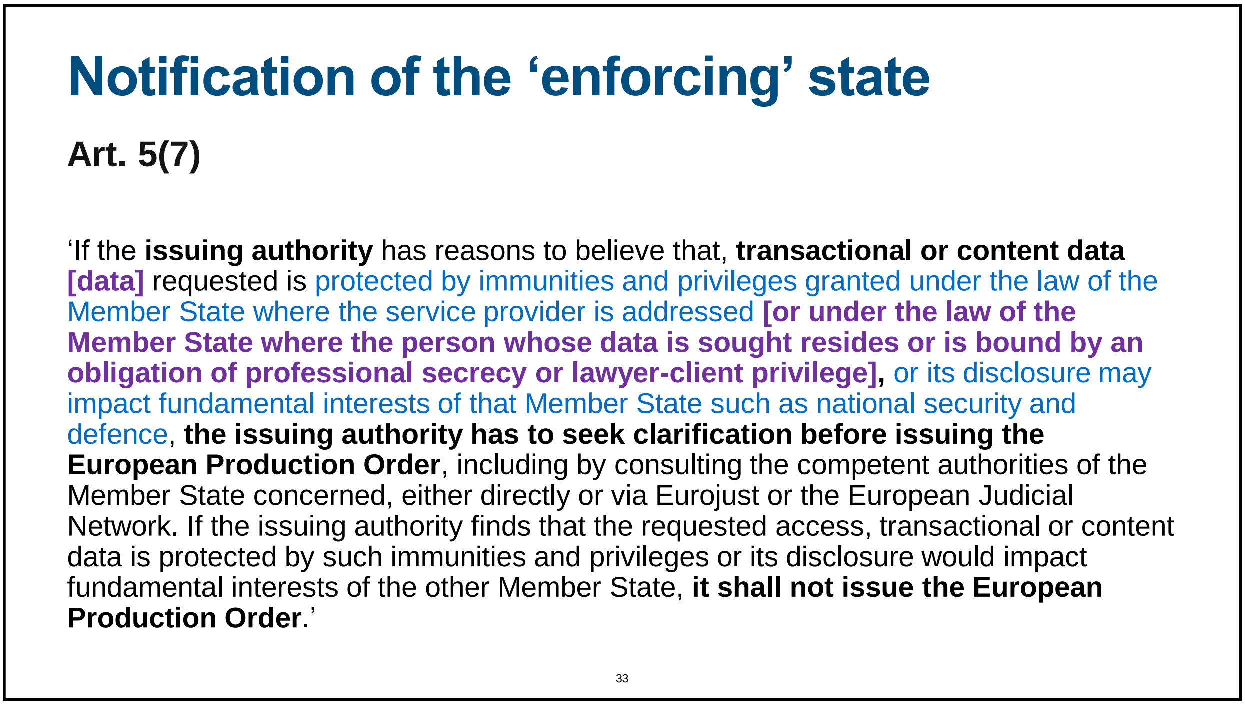
31

31

# Notification obligation

32

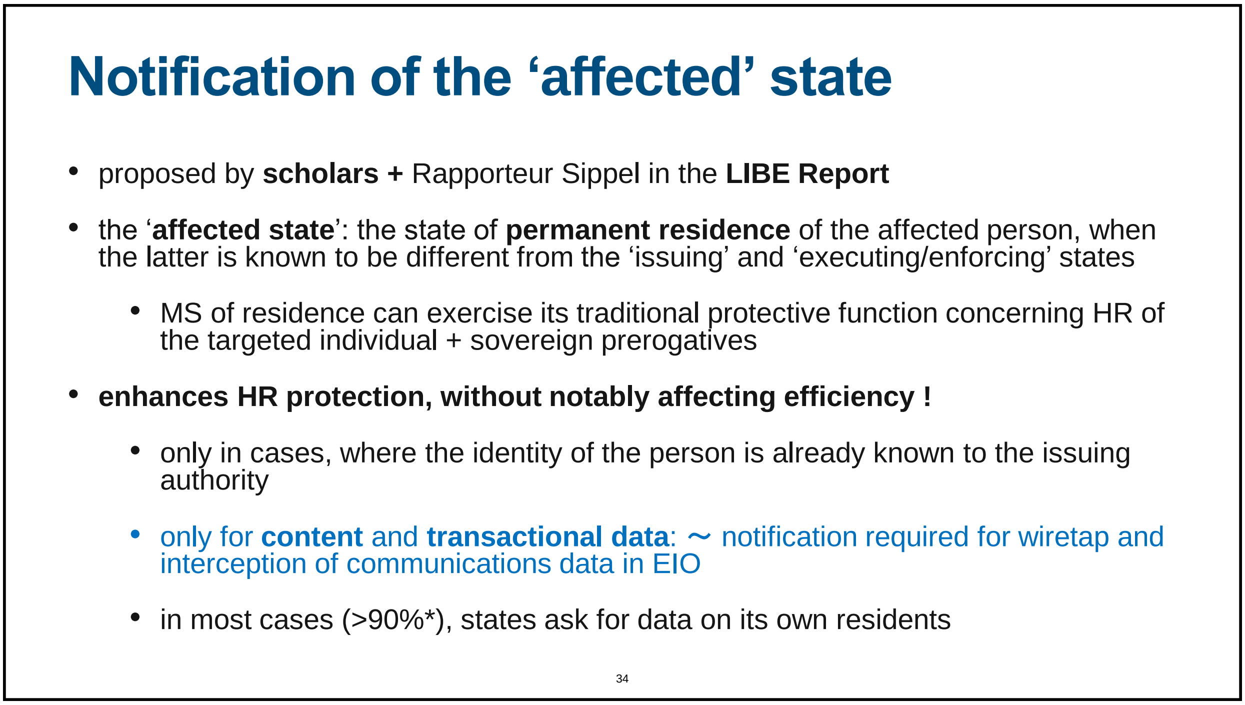
32



# Notification of the ‘enforcing’ state

## Art. 5(7)

‘If the **issuing authority** has reasons to believe that, **transactional or content data** **[data]** requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed **[or under the law of the Member State where the person whose data is sought resides or is bound by an obligation of professional secrecy or lawyer-client privilege]**, or its disclosure may impact fundamental interests of that Member State such as national security and defence, **the issuing authority has to seek clarification before issuing the European Production Order**, including by consulting the competent authorities of the Member State concerned, either directly or via Eurojust or the European Judicial Network. If the issuing authority finds that the requested access, transactional or content data is protected by such immunities and privileges or its disclosure would impact fundamental interests of the other Member State, **it shall not issue the European Production Order**.’



# Notification of the ‘affected’ state

- proposed by **scholars +** Rapporteur Sippel in the **LIBE Report**
- the ‘**affected state**’: the state of **permanent residence** of the affected person, when the latter is known to be different from the ‘issuing’ and ‘executing/enforcing’ states
  - MS of residence can exercise its traditional protective function concerning HR of the targeted individual + sovereign prerogatives
- **enhances HR protection, without notably affecting efficiency !**
  - only in cases, where the identity of the person is already known to the issuing authority
  - only for **content** and **transactional data**: ~ notification required for wiretap and interception of communications data in EIO
  - in most cases (>90%*), states ask for data on its own residents

## Additional rights/safeguards-focused elements of the EP proposal

- **default notification of the person whose data are being sought** (judicial gag order)
- **defence rights**: the issuing of an EPO (or preservation order) may also be requested on behalf of a suspected/accused person ... in accordance with national criminal procedures (Art. 1a)
- **purpose limitation**: 'Electronic information obtained in accordance with this Regulation shall not be used for the purpose of proceedings other than those for which it was obtained in accordance with this Regulation, except for where there is an imminent threat to the life or physical integrity of a person.' (Art. 11a)
- rules on **erasure** and **admissibility** of information gathered (Arts. 15, 16)

## Thank you for you attention!

m.galic@vu.nl

# OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

## Special investigation techniques: a new evidentiary frontier for the judge

Seminar organized by ERA, in cooperation with the Polish National School of Judiciary and Public Prosecution - Cracow, 24-25 March 2022

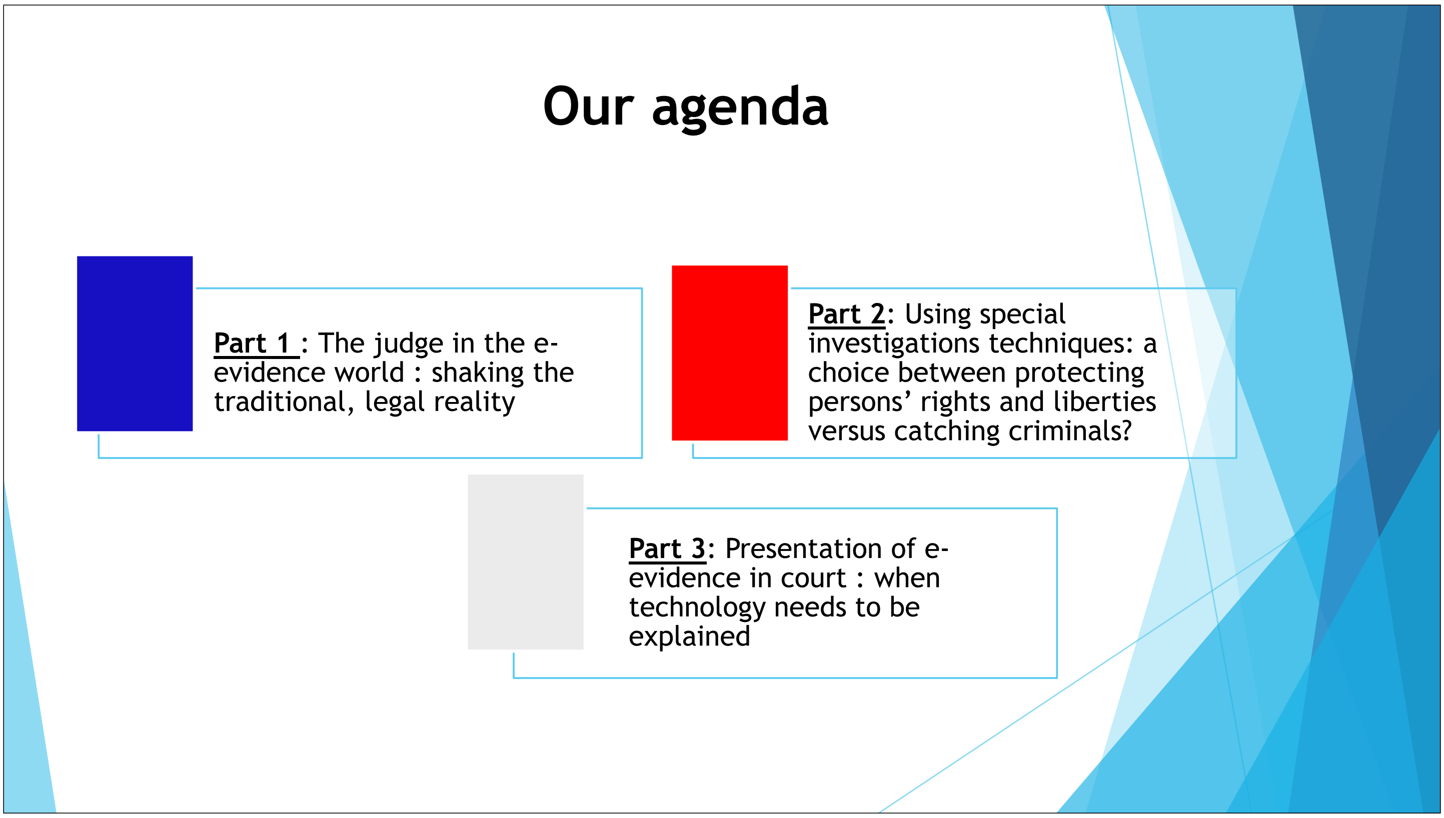
**Emmanuelle Legrand**

**French prosecutor/judge – AI project manager, French Ministry of Economy & Finance**

***Formerly public prosecutor, investigating judge, trial judge, liaison prosecutor in Western Balkans, and seconded national expert to the European Commission (DG JUST)***

*Views expressed in this presentation are personal views of the author and do not reflect the views of any institution.*

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



# Our agenda

**Part 1** : The judge in the e-evidence world : shaking the traditional, legal reality

**Part 2**: Using special investigations techniques: a choice between protecting persons’ rights and liberties versus catching criminals?

**Part 3**: Presentation of e-evidence in court : when technology needs to be explained

**Part 1** : The judge in the e-evidence world : shaking the traditional, legal reality

**Questions to the participants**:

1) if you are between 30ish and 50ish, you are a judge/prosecutor/lawyer, have you ever been taught in your initial training how a DDoS attack works?

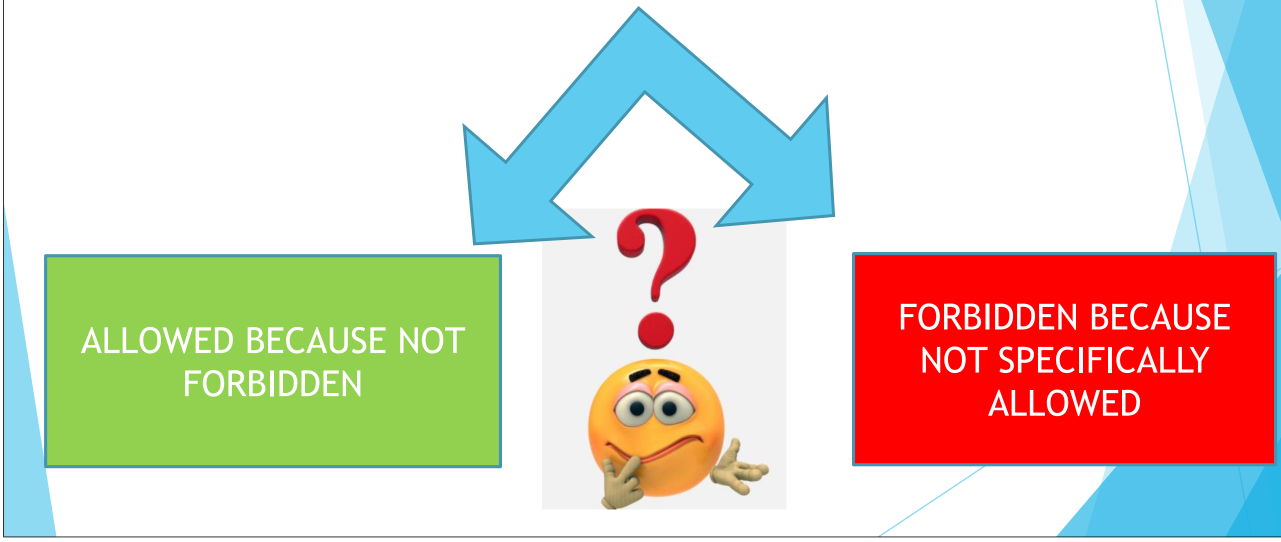
2) Another try : Have you ever heard about these strange acronyms in your legal training … CGN? IPV4 or 6? IoT? BEC?

3) Let's think of our future colleagues: Have you ever wondered how civil or criminal liability will be taught when we have autonomous AI systems, such as autonomous cars?

| **« Traditional » investigating/judicial reality** | **Digital reality** |
|---|---|
| • Time of commission of the crime | • Exchange of data easier and quicker (illicit downloading, sharing of child porn images, large-scale dissemination of malwares …) |
| • Consequences of the crime visible or rapidly known | • Detection of crime more difficult |
| • Criminal law resting on territoriality principle for judicial authorities and on respect of sovereignty principle | • International criminal phenomena across borders and need for swift investigations at the international level |
| • Traces left by the perpetrator :<br>- targeted searches according to the nature of the crime<br>- Difficult to erase<br>- Quite clear interpretation of evidence | • Digital evidence - difficult to identify :<br>- demultiplied storage capacities/devices<br>- erasable, volatile (1 clic to erase all)<br>- Decryption et interpretation sometimes difficult b/c technical |
| • Incompressible time for investigations to collect enough evidence | • Volatility of electronic evidence (can be erased in seconds) |
| • Capacities/expertise of investigators and judges/prosecutors: criminal law, procedural law | • New technical capacities required to lead investigations and to interpret pieces of evidence |
| • Procedural issues - Sometimes written procedure - paper | • 1 HD of 12 Gb = a pile of paper as high as the Eiffel Tower // 1Tb = 1000 Gb = 35 millions of pages |
| • Places of investigation quite easily identified | • Places of investigation not as easy to identify |

# Often, when collecting e-evidence, the first question may be:

**What is <u>NOT</u> specifically foreseen in the law is :**



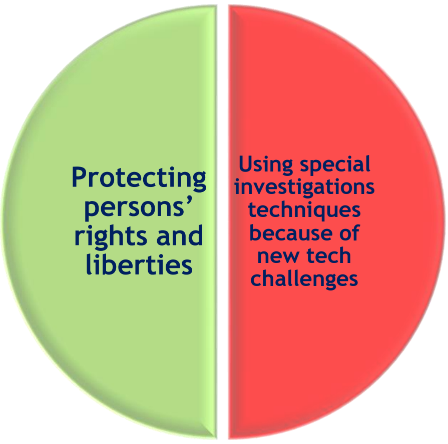
ALLOWED BECAUSE NOT FORBIDDEN

FORBIDDEN BECAUSE NOT SPECIFICALLY ALLOWED

# Main consequences for the judge

- **More important/active role in « drawing the lines » in the investigations** (between what is authorized and what is prohibited)
- **Traditional evidentiary expectations may not always be fully/easily met**
- **How far can you trust technologies?** *(eg. Who says this IP address means I did use the computer in my house where I live with 2 other persons?)*
- **Technical help needed to understand/read/interpret the evidence**

**Part 2**: Using special investigations techniques: a choice between protecting persons’ rights and liberties versus catching criminals?



Protecting persons’ rights and liberties

Using special investigations techniques because of new tech challenges

## No common legal definition of special investigations techniques

❑ **Definition proposed by the Council of Europe:**

**« techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons »**

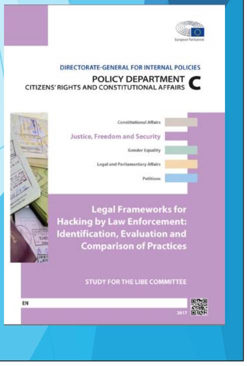
*(Recommandation Rec (2005)10 on special investigations techniques in relation to serious crimes including acts of terrorism)*

## ”[Legal] hacking by law enforcement” / remote access to computer data

❖ **Comparative study for the LIBE Committee of the European Parliament:**

*« Legal frameworks for hacking by law enforcement: identification, evaluation, and comparison of practices » (2017)*

[*https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf*](https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf)



DIRECTORATE-GENERAL FOR INTERNAL POLICIES
POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs
Justice, Freedom and Security
Gender Equality
Legal and Parliamentary Affairs
Petitions

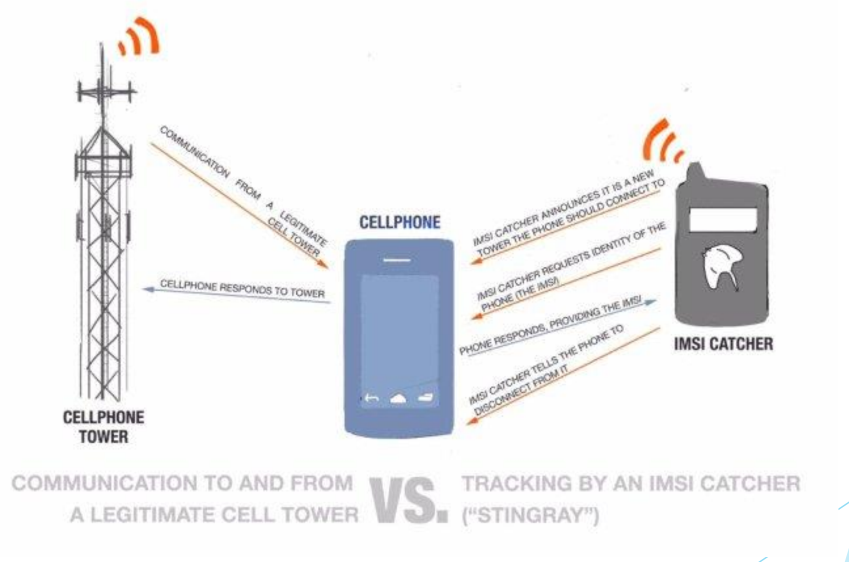
Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices

STUDY FOR THE LIBE COMMITTEE

EN

2017

## IMSI Catcher


CELLPHONE TOWER
COMMUNICATION FROM A LEGITIMATE CELL TOWER
CELLPHONE RESPONDS TO TOWER
CELLPHONE
IMSI CATCHER ANNOUNCES IT IS A NEW TOWER THE PHONE SHOULD CONNECT TO
IMSI CATCHER REQUESTS IDENTITY OF THE PHONE (THE IMSI)
PHONE RESPONDS, PROVIDING THE IMSI
IMSI CATCHER TELLS THE PHONE TO DISCONNECT FROM IT
IMSI CATCHER
COMMUNICATION TO AND FROM A LEGITIMATE CELL TOWER
VS.
TRACKING BY AN IMSI CATCHER ("STINGRAY")

* Source: https://techsecurity.news/tag/imsi-catcher

# Facing technological challenges… how/what/who/where?

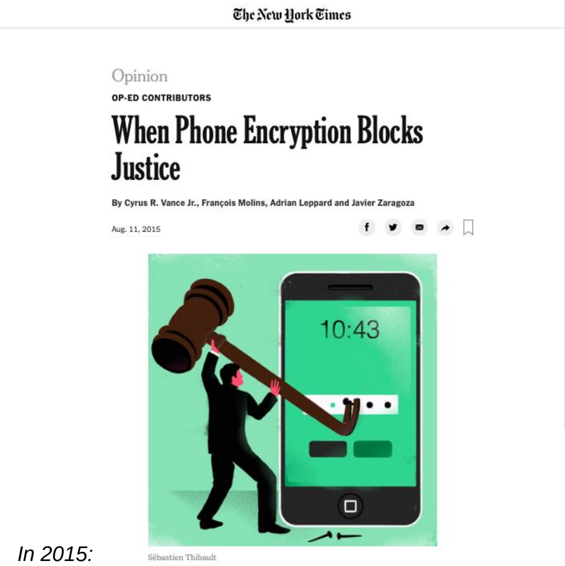
## Going dark phenomenon – how?

- « **“Going Dark”** is a term used by law enforcement agencies to describe their **decreasing ability to lawfully access and examine evidence at rest on devices and evidence in motion across communications networks.** The rapid growth of new services and technologies means that an increasing amount of evidence that resides on criminals’ computers and mobile devices is beyond the reach of law enforcement, evidence that law enforcement needs to investigate illegal activity and prosecute criminals. »

*IACP (International association of chiefs of police) Summit Report. 2015. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence.*

*https://www.theiacp.org/sites/default/files/all/i-j/IACPSummitReportGoingDark.pdf*

# Encryption- what?



The New York Times

Opinion

OP-ED CONTRIBUTORS

**When Phone Encryption Blocks Justice**

By Cyrus R. Vance Jr., François Molins, Adrian Leppard and Javier Zaragoza

Aug. 11, 2015

Sébastien Thibault

*In 2015:*
*Cyrus R. Vance Jr., Manhattan district attorney;*
*François Molins, Paris chief prosecutor;*
*Adrian Leppard, commissioner of the City of London Police;*
*Javier Zaragoza, chief prosecutor of the High Court of Spain.*

« (…) The new Apple encryption would not have prevented the N.S.A.’s mass collection of phone-call data or the interception of telecommunications, as revealed by Mr. Snowden. There is no evidence that it would address institutional data breaches or the use of malware. And we are not talking about violating civil liberties — we are talking about the ability to unlock phones pursuant to lawful, transparent judicial orders.
In the United States, Britain, France, Spain and other democratic societies, the legal system gives local law enforcement agencies access to places where criminals hide evidence, including their homes, car trunks, storage facilities, computers and digital networks.

**Carved into the bedrock of each of these laws is a balance between the privacy rights of individuals and the public safety rights of their communities.** For our investigators to conduct searches in any of our jurisdictions, a local judge or commissioner must decide whether good cause exists. None of our agencies engage in bulk data collection or other secretive practices. We engage in targeted requests for information, authorized after an impartial, judicial determination of good cause, in which both proportionality and necessity are tested (…) »

**« (…) The new encryption policies of Apple and Google have made it harder to protect people from crime. We support the privacy rights of individuals.** But in the absence of cooperation from Apple and Google, regulators and lawmakers in our nations must now find an appropriate balance between the marginal benefits of full-disk encryption and the need for local law enforcement to solve and prosecute crimes. **The safety of our communities depends on it. »**

# Carrier grade Nat – who?

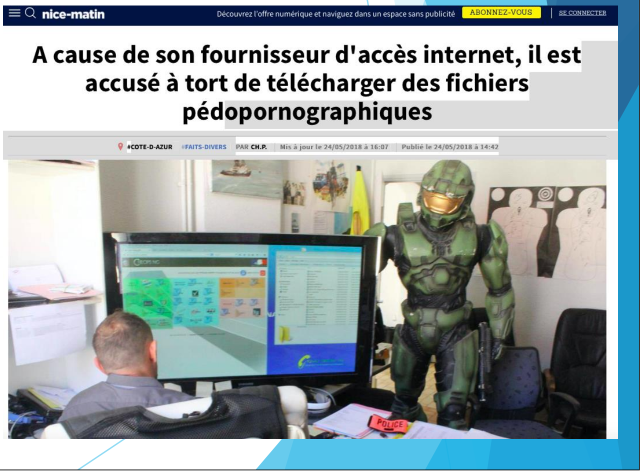
## ARE YOU SHARING THE SAME IP ADDRESS AS A CRIMINAL? LAW ENFORCEMENT CALL FOR THE END OF CARRIER GRADE NAT (CGN) TO INCREASE ACCOUNTABILITY ONLINE

17 Oct 2017

Press Release

Europol and the Estonian Presidency of the EU Council address the serious online capability gap in law enforcement efforts to investigate and attribute crime created by CGN technologies.

```
DHCPREQUEST on ens257 to 192.168.0.1
DHCPACK from 192.168.0.1
DHCPACK from 192.168.0.1
bound to 192.168.0.216
bound to 192.168.0.216
(7181): <info> (ens257): DHCPv4
(7181): <info>  address 192.168.0.216
(7181): <info>  plen 24 (255.255.255.0)
(7181): <info>  gateway 192
```

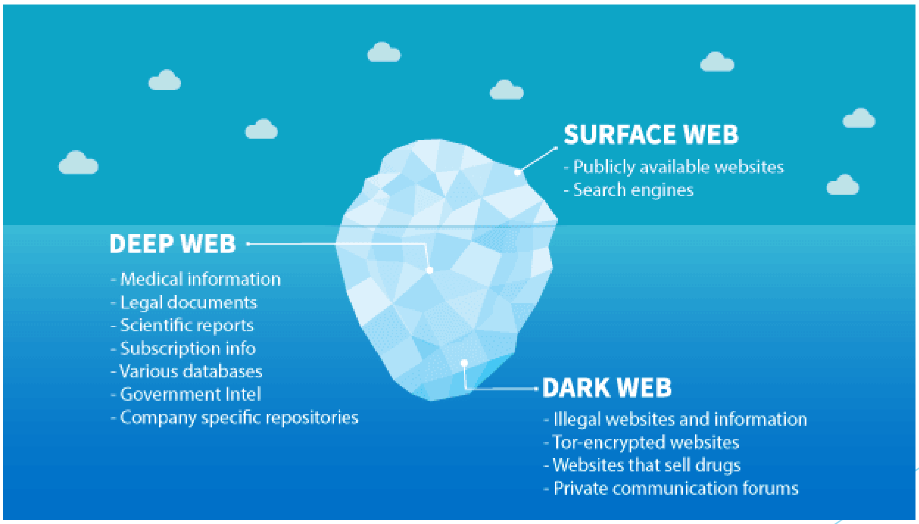


nice-matin
Découvrez l'offre numérique et naviguez dans un espace sans publicité
ABONNEZ-VOUS
SE CONNECTER

**A cause de son fournisseur d'accès internet, il est accusé à tort de télécharger des fichiers pédopornographiques**

#COTE-D-AZUR #FAITS-DIVERS PAR CH.P. | Mis à jour le 24/05/2018 à 16:07 | Publié le 24/05/2018 à 14:42

# E-evidence from the dark web- where?



* Source: https://nitrocdn.com/yvAWAwIUuhWCbexUJQJczTYwPUYbZGXM/assets/static/optimized/rev-39255f4/wp-content/uploads/dark-web-surface-web-graphic.png

GOING TO THE DARK WEB/using Tor IS ILLEGAL

WRONG

USING THE DARK WEB FOR ILLEGAL ACTIVITIES IS ILLEGAL

RIGHT

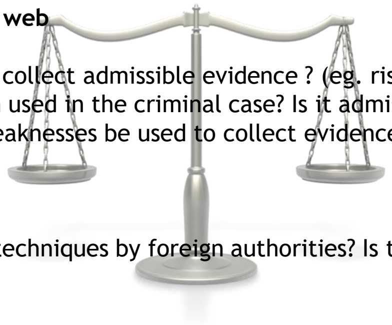
**Questions from the judge**: Where does the evidence come from? Who could access the information? How did the police get access to it? Is the information found a crime in itself or does it come from a crime, and if so, which one? Were they undercover? Did they obtain the evidence loyally? Did the officers have the authorization/capacity to act as they did online? How did you identify that nickname?

## A few questions raised when investigating on the dark web:

**Interesting report available at:**
https://www.rand.org/pubs/research_reports/RR2704.html

**Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web**

- **Anonymity (ToR)- cryptocurrencies**
  - how to make sure of the identity of the perpetrator?
  - How do I discriminate data when I do not know who is who? Can I ? Risks for admissibility?
- **Crimes committed through the dark web**
  - What legal provisions to use to collect admissible evidence ? (eg. risk of entrapment; type of data)
  - How is intelligence information used in the criminal case? Is it admissible?
  - May softwares' or networks' weaknesses be used to collect evidence ?
- **Cross-jurisdictional issues :**
  - What about jurisdiction?
  - What about the use of special techniques by foreign authorities? Is the evidence admissible before your judge ?

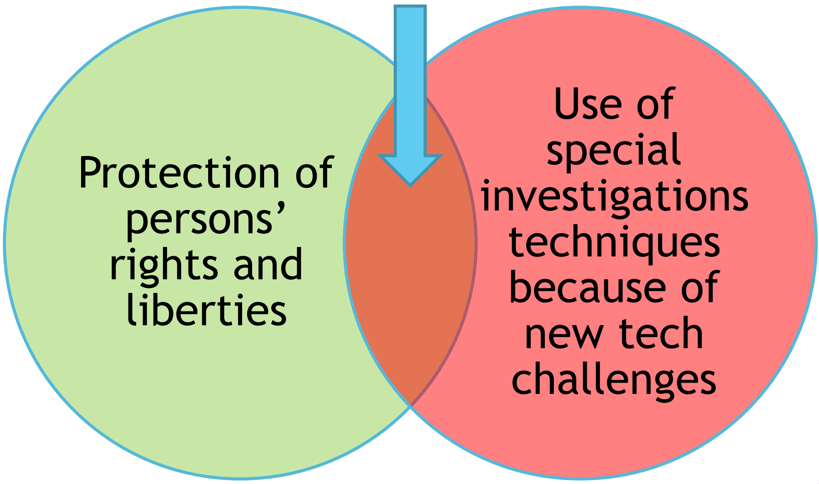


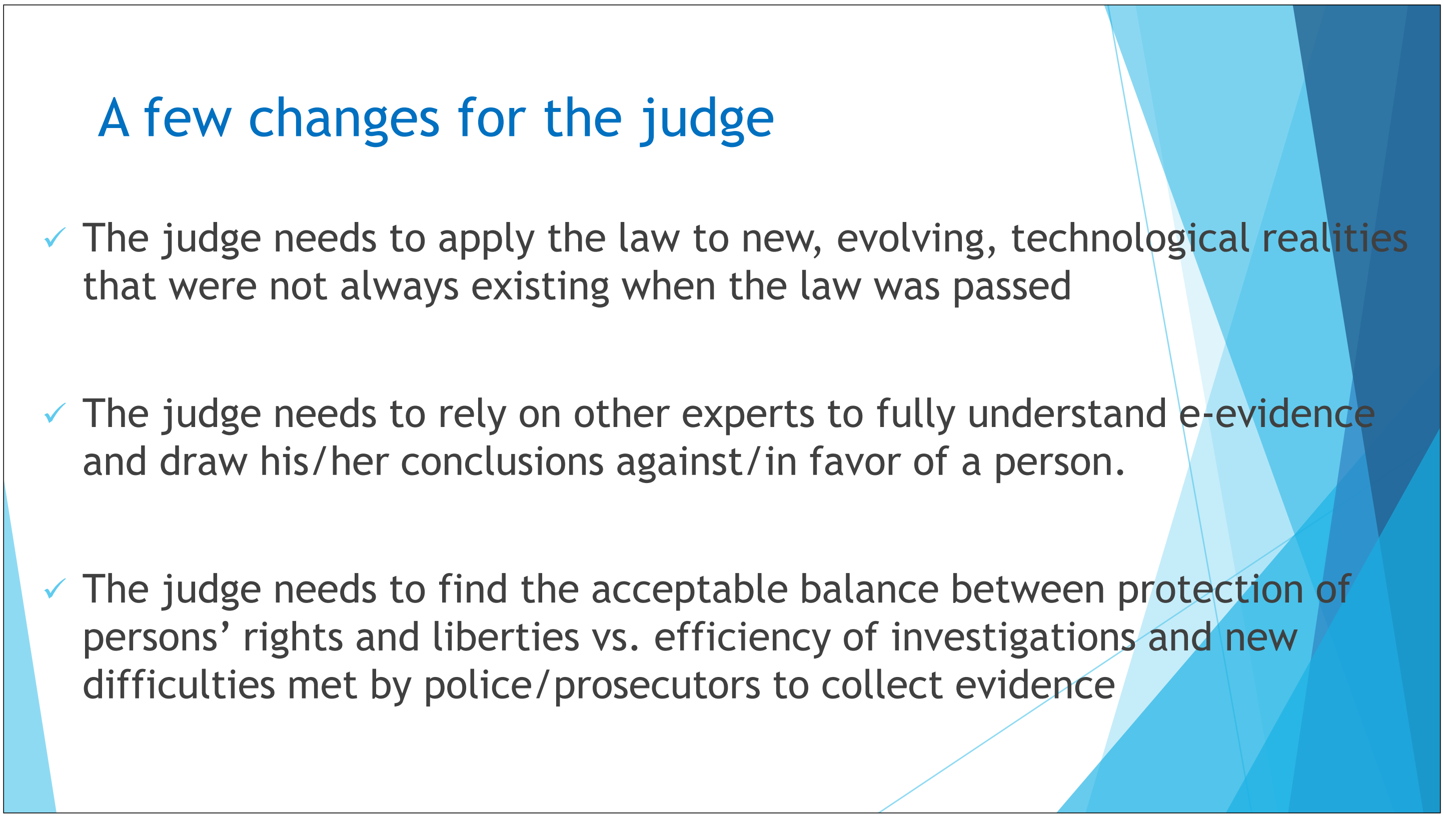
# E-evidence from darknet/websites/social networks – a few more questions from the judge :

- Where did you get access to this content ?
- Can you please print it for my case?
- How do you want me to read these unreadable logs. What am I supposed to conclude from that ?
- Did you respect international agreements to get this information ?
- How did you obtain the information from the service provider abroad ?
- Were you undercover/did you act under a specific procedural framework?
- Was it a public or private profile ?
- How did you intercept the flow of messaging ? Did you check in what country the persons were to do that ?
- How did you make the link between this nickname and that person?
- How come you cannot provide me with the emails? Didn't you ask the service provider?
- Did you just copy the data? What makes it reliable if it's just a copy?
- Is the website still functioning? Can I really order to seize it?
- How can you be sure this is a true/fake profile?
- - You needed to provide me with the evidence from the country where the website is hosted!

  - I could not, this comes from North Korea. How could we get it, judge? They don't cooperate!

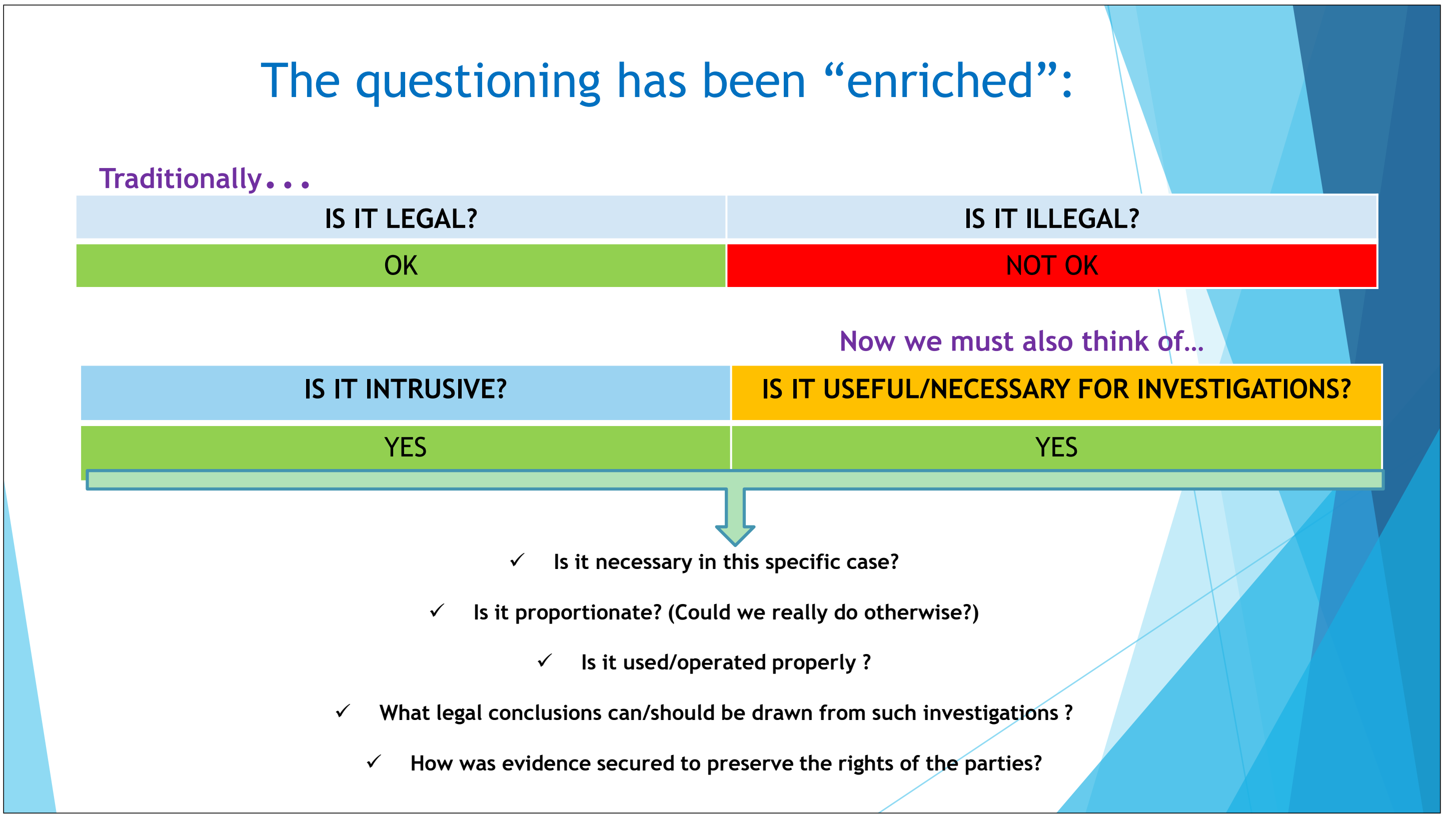
Using special investigations techniques: protecting persons' rights and liberties **WHILE** catching criminals


Protection of persons' rights and liberties
Use of special investigations techniques because of new tech challenges



# A few changes for the judge

- ✓ The judge needs to apply the law to new, evolving, technological realities that were not always existing when the law was passed
- ✓ The judge needs to rely on other experts to fully understand e-evidence and draw his/her conclusions against/in favor of a person.
- ✓ The judge needs to find the acceptable balance between protection of persons' rights and liberties vs. efficiency of investigations and new difficulties met by police/prosecutors to collect evidence



# The questioning has been "enriched":

Traditionally...

| IS IT LEGAL? | IS IT ILLEGAL? |
|---|---|
| OK | NOT OK |

Now we must also think of…

| IS IT INTRUSIVE? | IS IT USEFUL/NECESSARY FOR INVESTIGATIONS? |
|---|---|
| YES | YES |

- ✓ Is it necessary in this specific case?
- ✓ Is it proportionate? (Could we really do otherwise?)
- ✓ Is it used/operated properly ?
- ✓ What legal conclusions can/should be drawn from such investigations ?
- ✓ How was evidence secured to preserve the rights of the parties?

## **Part 3**: Presentation of e-evidence in court : when technology needs to be explained

- Origin and integrity of data and methodology about collection of e-evidence are key elements (real/fake; chain of custody; jurisdiction issues)
- Avoid the « black box » situation (training of judges; presentation of evidence by the prosecutor in an adequate format; definition of technical terms; technical possibilities in the courtroom to understand the evidence; explanations by experts in a not-too-technical manner)
- Accept some part of uncertainty with the technology (?)
- Balance the rights of the defense vs. the risk to make too much information public about investigation techniques
- Accept that uncertain interpretation of the law will often occur in the e-evidence world.

## Any interesting case law related to e-evidence in your courts? Please share, I am interested!

**Emmanuelle Legrand**

**emmanuelle.legrand@finances.gouv.fr /or/ legrandepro@orange.fr**

# Trial considerations: methods of presentation and admissibility tests

30 YEARS ERA

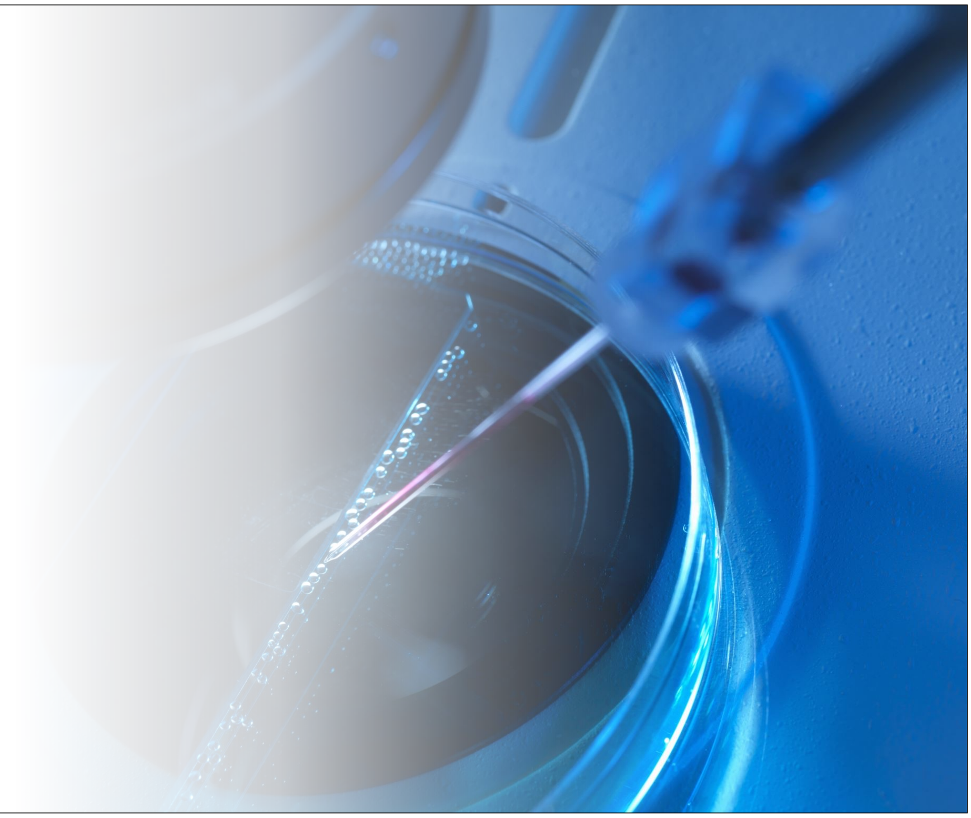
*The importance of the chain of custody in handling evidence and best practices*

*Cracow, 24-25 March 2022*

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

# Agenda

1. *Refresher on the Electronic Evidence*
2. *Trial preparation considerations*
3. *Trial presentation considerations*
4. *Investigation case specific considerations*
5. *Case examples*



# Refresher on the electronic evidence

## Definitions

**Evidence**

- 'any species of proof or probative matter, legally presented at the trial of an issue, by the act of parties and through the medium of witnesses, records, documents, exhibits, concrete objects, etc. for the purpose of inducing belief in the minds of the court or jury as their contention'

**Electronic Evidence?**

- Evidence emanating from an electronic device
- Generally admissible into legal proceedings

*Source: Black's Law Dictionary*

# Definitions

**Electronic Evidence Definitions:**

**1. Council of Europe Electronic Evidence Guide**:

*”Any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings”*

**2. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (2018):**

*”Electronic evidence means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data”*

**3. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (2019):**

*“Electronic evidence” means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network”*

# Differences

## Electronic Evidence

- **Not different** from traditional evidence
- **Necessary** for the party introducing it into legal proceedings, **to be able to demonstrate that it is no more and no less than it was**, when it came into their possession
- In other words, **it shows that no changes, deletions, additions or other alterations have taken place**

# Differences

## Electronic Evidence

- **Nature of data and information** held in electronic form makes it easier to manipulate than traditional forms of evidence
- **Creates specific issues for the justice system** and requires that the handling of such data is carried out in a manner that ensures the continued integrity of the information may be maintained and proved.

# Budapest Convention definitions

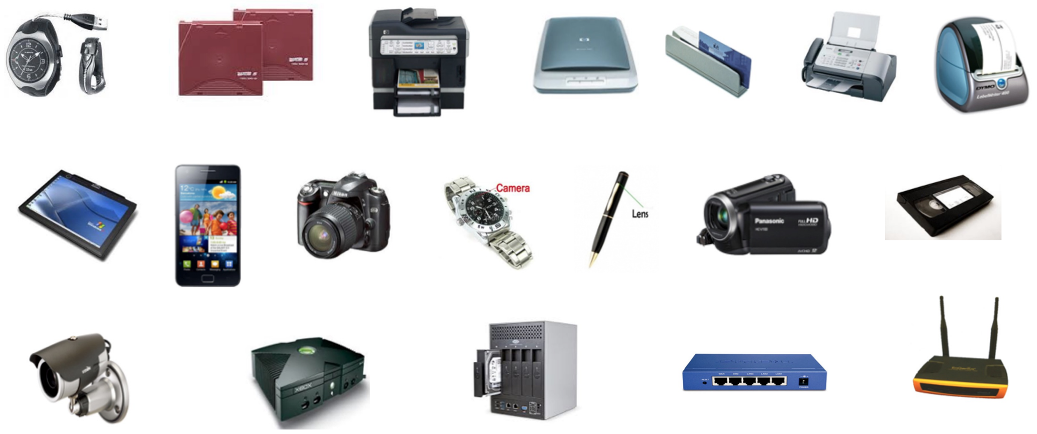
## Computer System

- any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic data processing

## Computer Data

- any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function

## Sources



# Chain of Custody and Evidence

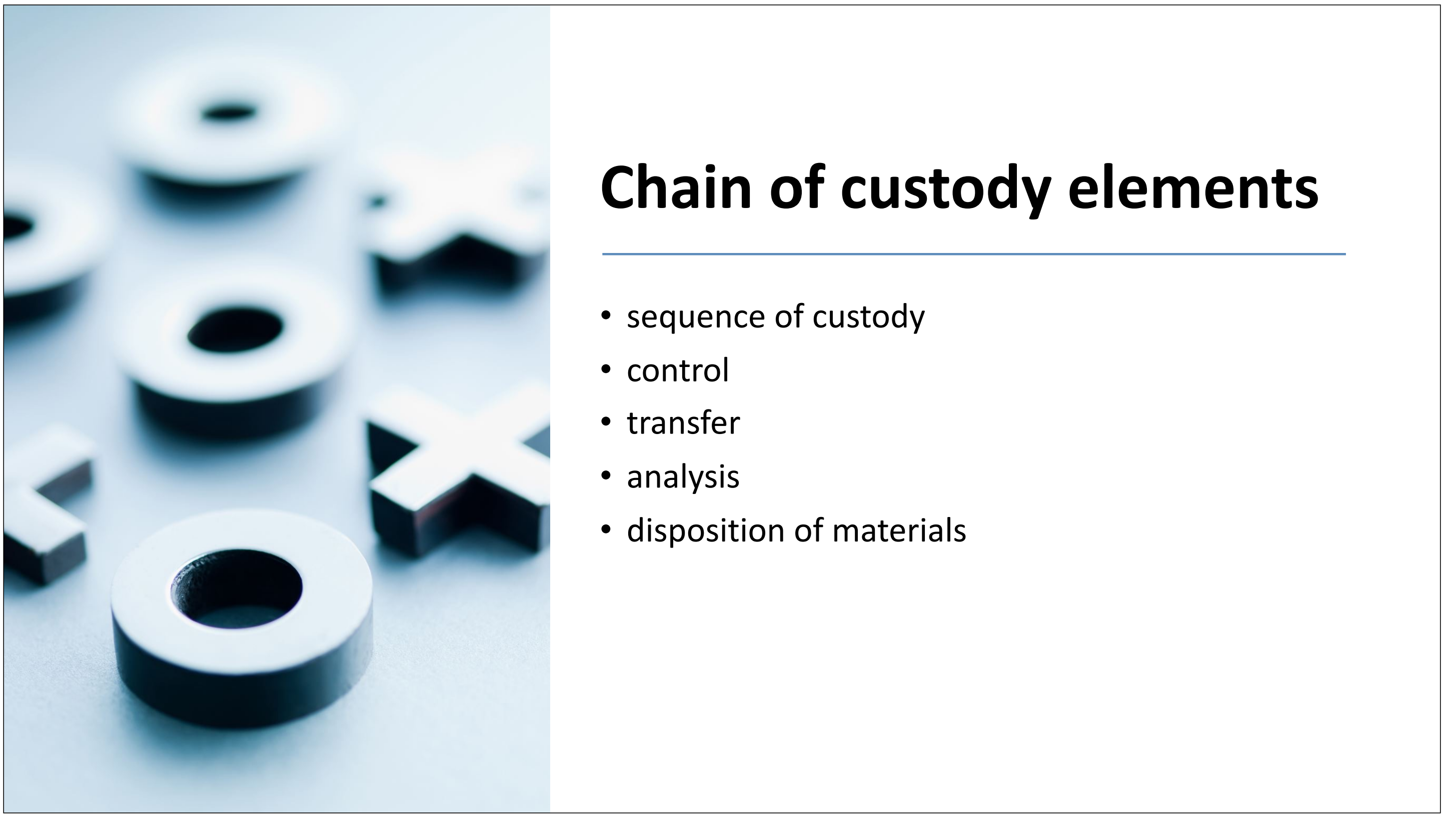
### Chain of Custody Definition:

Chain of custody, in legal contexts, is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence.

### Chain of Evidence Definition:

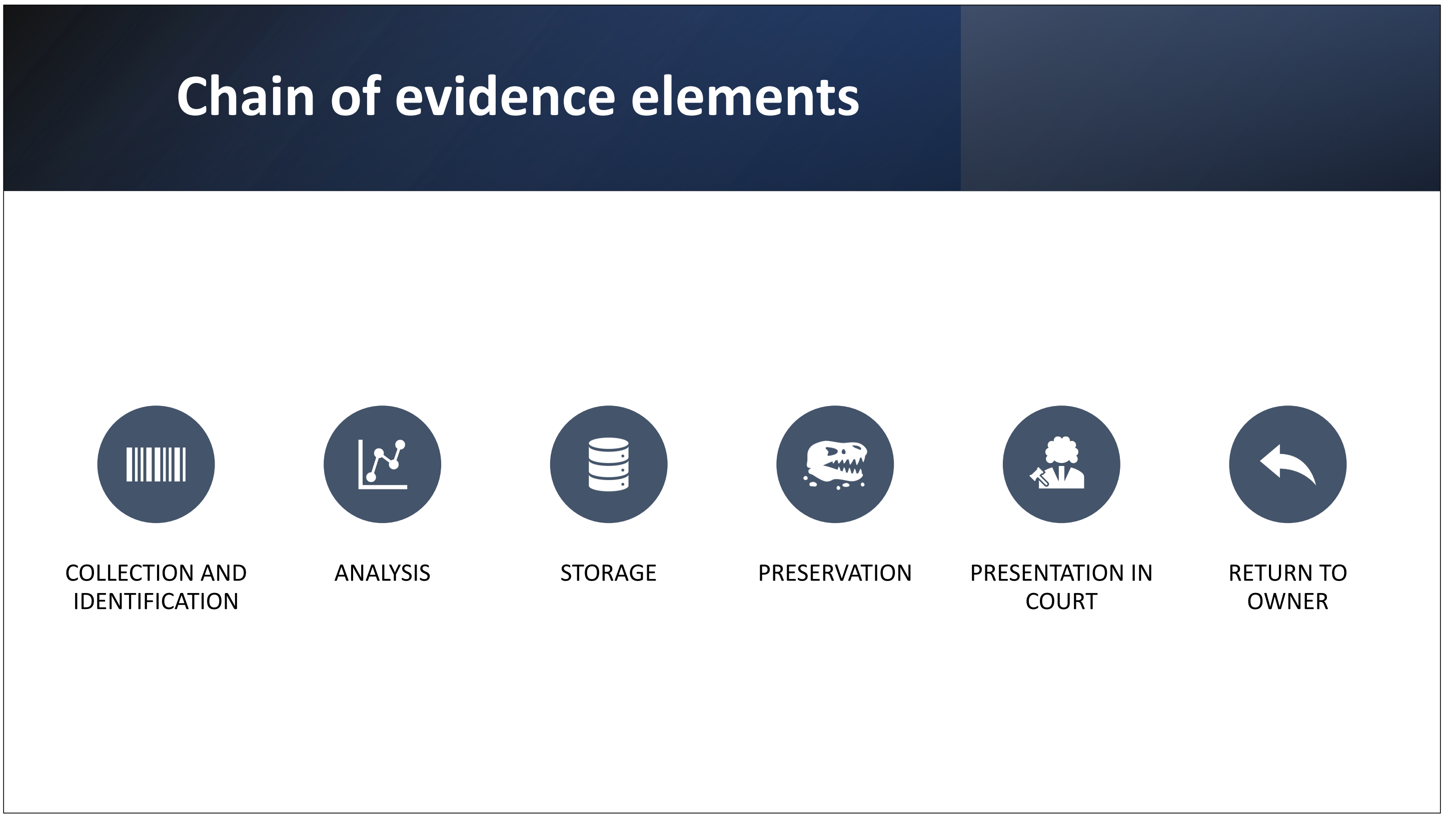
A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence.

The “sequencing” of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner.



# Chain of custody elements

- sequence of custody
- control
- transfer
- analysis
- disposition of materials



# Chain of evidence elements

COLLECTION AND IDENTIFICATION

ANALYSIS

STORAGE

PRESERVATION

PRESENTATION IN COURT

RETURN TO OWNER

# Most important investigation Electronic Evidence Principles

## 1. Data Integrity

***‘No action taken should change electronic devices or media, which may subsequently be relied upon in court’***

✓ Aim is to make no change

✓ OIC is responsible for integrity & the forensic chain

✓ Data on a ‘live’ machine may change
- Change should cause the least impact
- Undertaken in particular manner
- By person qualified to do so

# Most important investigation Electronic Evidence Principles

## 2. Legality

***‘The person and agency in charge of the case are responsible for ensuring that the law, the general forensic and procedural principles are adhered to. This applies to the possession of and access to electronic evidence’***

States should have their own procedural system in place

Need to ensure processes & training in place

# Considerations

- **Handled** - by specialists
- **Evolution** - sources change quickly
- **Procedures** - proper tools & techniques
- **Admissibility** - follow guidance & principles
- **Authenticity** - must be tied to the incident
- **Completeness** - the whole story & not selective
- **Reliability** - no doubt about it
- **Believability** – be understandable
- **Proportionality** - meet the tests

# Electronic evidence and trial preparation considerations

## Preparation considerations

### 1. Fundamental definitions (Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings from 2019):

✓ ***Electronic evidence***

- "Electronic evidence" means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network.

✓ ***Metadata***

- "Metadata" refers to electronic information about other electronic data, which may reveal the identification, origin or history of the evidence, as well as relevant dates and times.

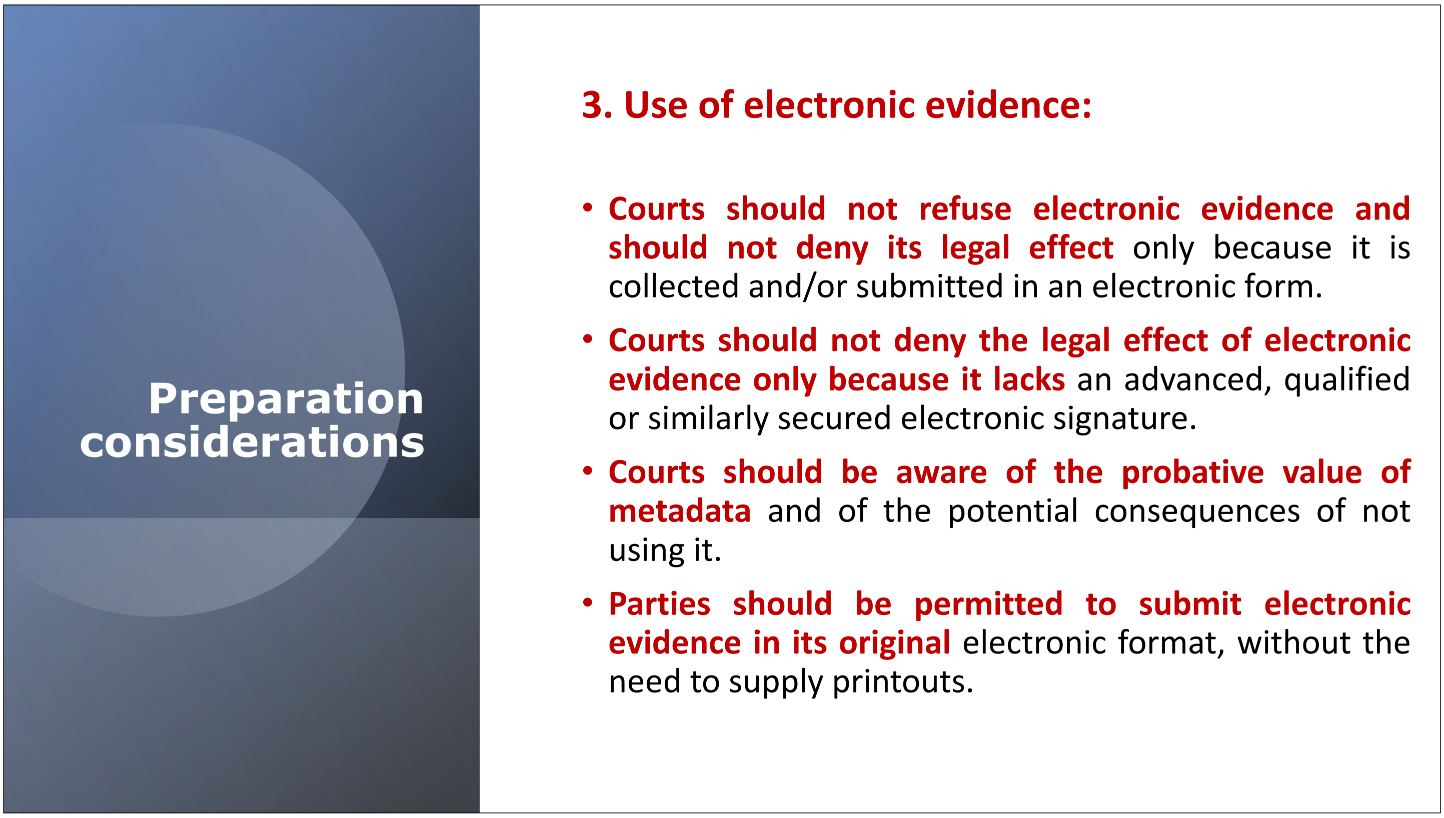
✓ ***Trust service***

- "Trust service" means an electronic service which consists of:
- *a.* the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or
- *b.* the creation, verification and validation of certificates for website authentication; or
- *c.* the preservation of electronic signatures, seals or certificates related to those services.

## Preparation considerations

### 2. Fundamental principles:

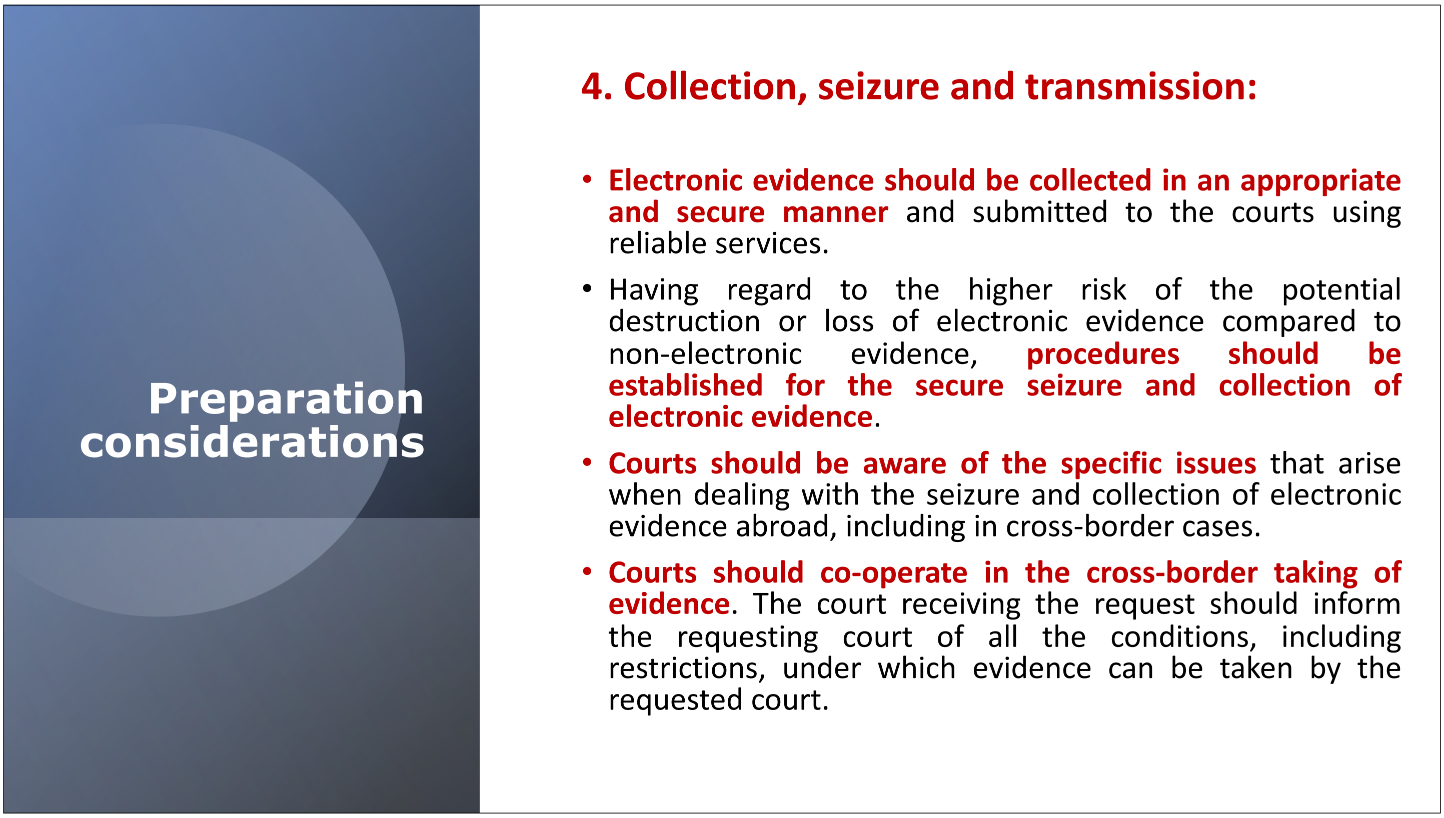
- **It is for courts to decide on the potential probative value** of electronic evidence in accordance with national law.
- **Electronic evidence should be evaluated in the same way as other types of evidence**, in particular regarding its admissibility, authenticity, accuracy and integrity.
- **The treatment of electronic evidence should not be disadvantageous** to the parties or give unfair advantage to one of them.



Preparation considerations

## 3. Use of electronic evidence:

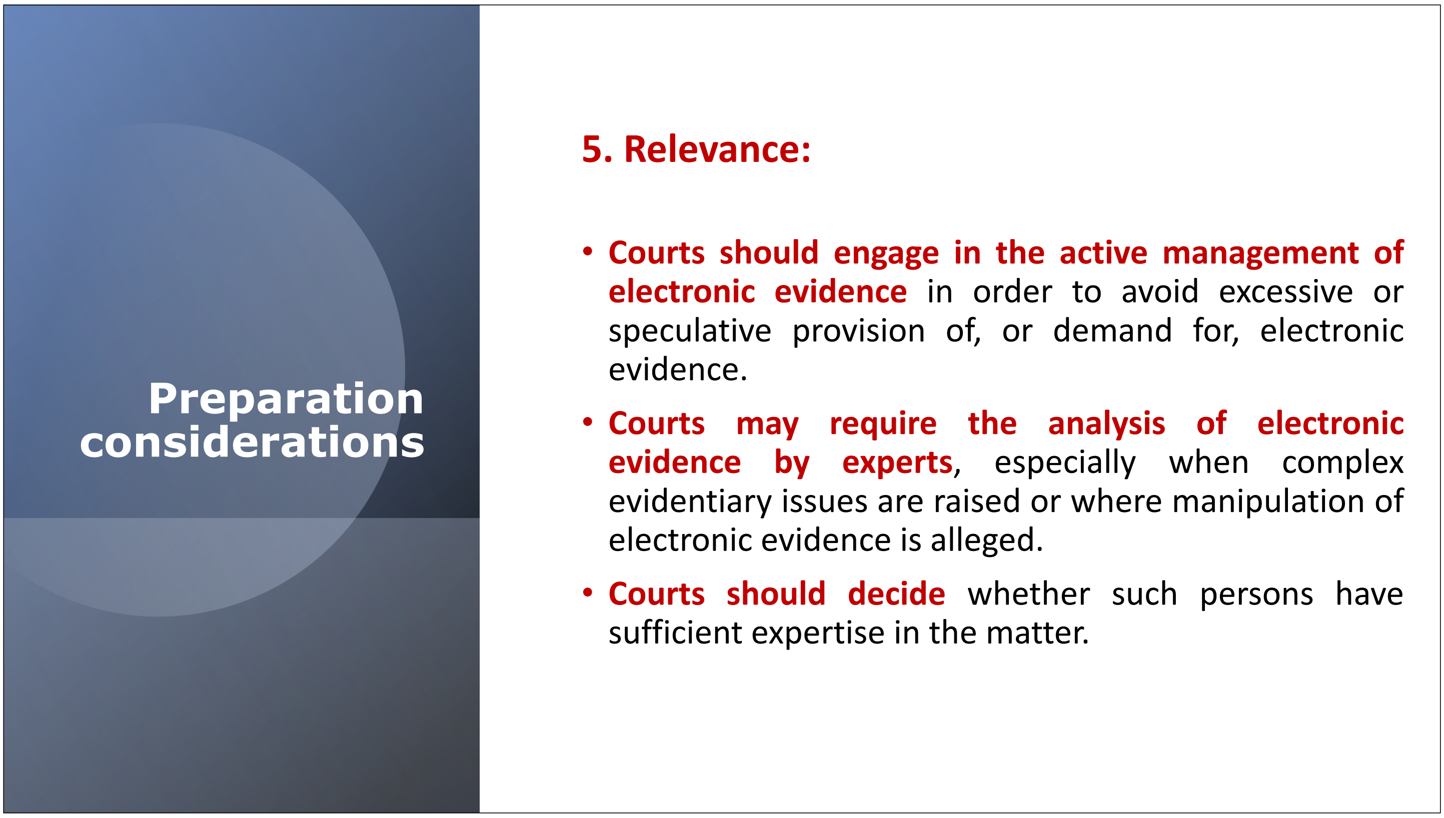
- **Courts should not refuse electronic evidence and should not deny its legal effect** only because it is collected and/or submitted in an electronic form.
- **Courts should not deny the legal effect of electronic evidence only because it lacks** an advanced, qualified or similarly secured electronic signature.
- **Courts should be aware of the probative value of metadata** and of the potential consequences of not using it.
- **Parties should be permitted to submit electronic evidence in its original** electronic format, without the need to supply printouts.



Preparation considerations

## 4. Collection, seizure and transmission:

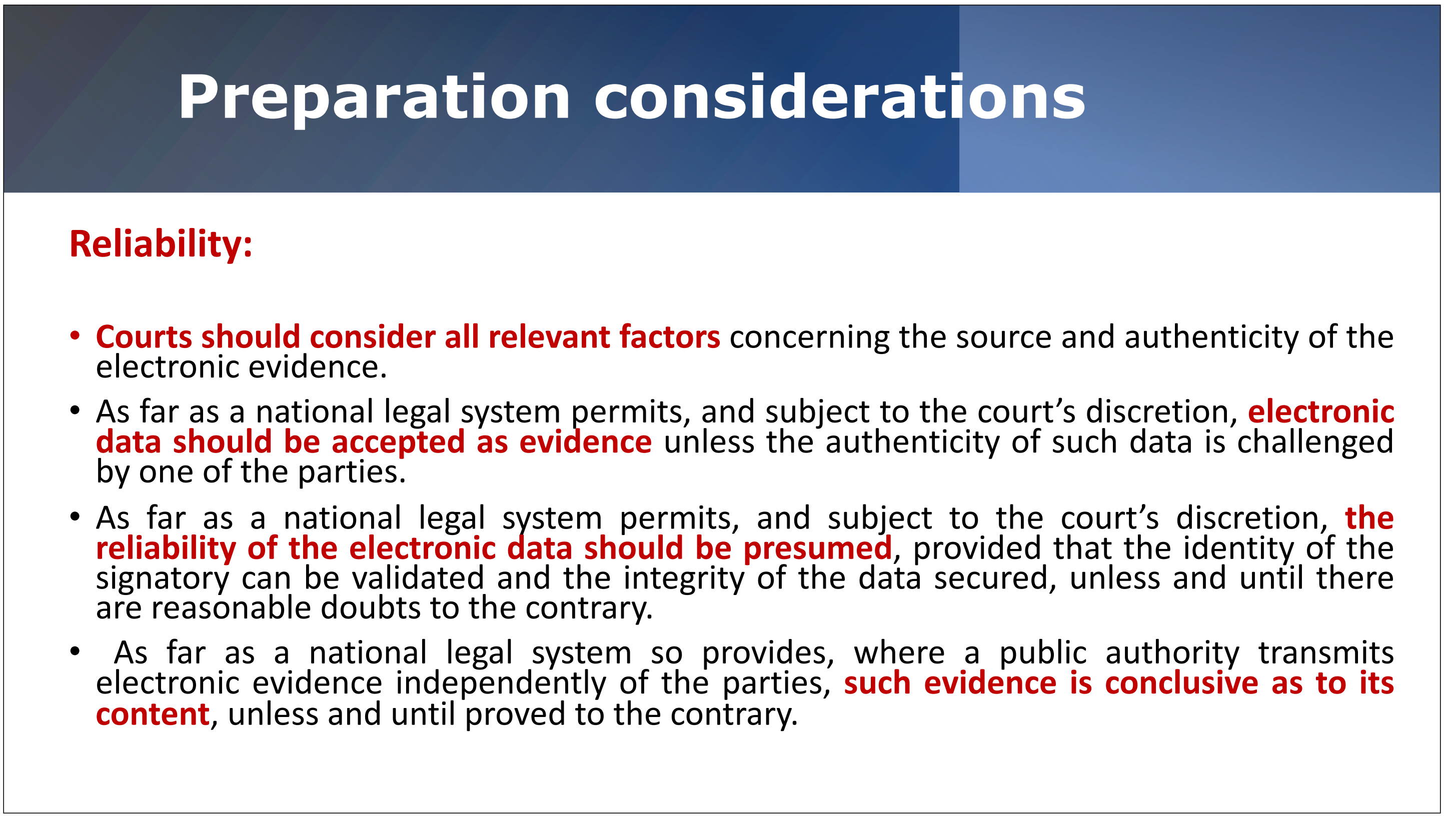
- **Electronic evidence should be collected in an appropriate and secure manner** and submitted to the courts using reliable services.
- Having regard to the higher risk of the potential destruction or loss of electronic evidence compared to non-electronic evidence, **procedures should be established for the secure seizure and collection of electronic evidence**.
- **Courts should be aware of the specific issues** that arise when dealing with the seizure and collection of electronic evidence abroad, including in cross-border cases.
- **Courts should co-operate in the cross-border taking of evidence**. The court receiving the request should inform the requesting court of all the conditions, including restrictions, under which evidence can be taken by the requested court.



## Preparation considerations

### 5. Relevance:

- **Courts should engage in the active management of electronic evidence** in order to avoid excessive or speculative provision of, or demand for, electronic evidence.
- **Courts may require the analysis of electronic evidence by experts**, especially when complex evidentiary issues are raised or where manipulation of electronic evidence is alleged.
- **Courts should decide** whether such persons have sufficient expertise in the matter.



# Preparation considerations

### Reliability:

- **Courts should consider all relevant factors** concerning the source and authenticity of the electronic evidence.
- As far as a national legal system permits, and subject to the court's discretion, **electronic data should be accepted as evidence** unless the authenticity of such data is challenged by one of the parties.
- As far as a national legal system permits, and subject to the court's discretion, **the reliability of the electronic data should be presumed**, provided that the identity of the signatory can be validated and the integrity of the data secured, unless and until there are reasonable doubts to the contrary.
- As far as a national legal system so provides, where a public authority transmits electronic evidence independently of the parties, **such evidence is conclusive as to its content**, unless and until proved to the contrary.

# Preparation considerations

## Storage and preservation:

- **Electronic evidence should be stored in a manner that preserves** readability, accessibility, integrity, authenticity, reliability and, where applicable, confidentiality and privacy.
- Electronic evidence **should be stored with standardized metadata** so that the context of its creation is clear.
- **The readability and accessibility of stored electronic evidence should be guaranteed over time**, taking into account the evolution of information technology.

# Preparation considerations

## Archiving:

- **Courts should archive electronic evidence** in accordance with national law.
- **Electronic archives should meet all safety requirements** and guarantee the integrity, authenticity, confidentiality and quality of the data as well as respect for privacy.
- The archiving of electronic evidence should **be carried out by qualified specialists.**
- **Data should be migrated to new storage media**, when necessary, in order to preserve accessibility to electronic evidence.

Electronic evidence and

Trial presentation considerations

# Presentation considerations

**Presentation of evidence principles:**

**Admissibility:** computer evidence is admissible if it conforms to a series of laws and rules that ensure it is acceptable to the court.

**Authenticity:** electronic evidence is no different to physical evidence, such as a document recorded on a piece of paper. It is necessary to ensure that the evidence is authentic.

**Convincing:** electronic evidence is dealt with in court in the same way as any other form of evidence. The prosecution will have to prove that the document is authentic, and its contents are admissible.

# Presentation considerations

**Explanation of the principles:**

**Electronic evidence is subject to the same rules** and laws that apply to documentary evidence

**The onus is on the prosecution** to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of law enforcement

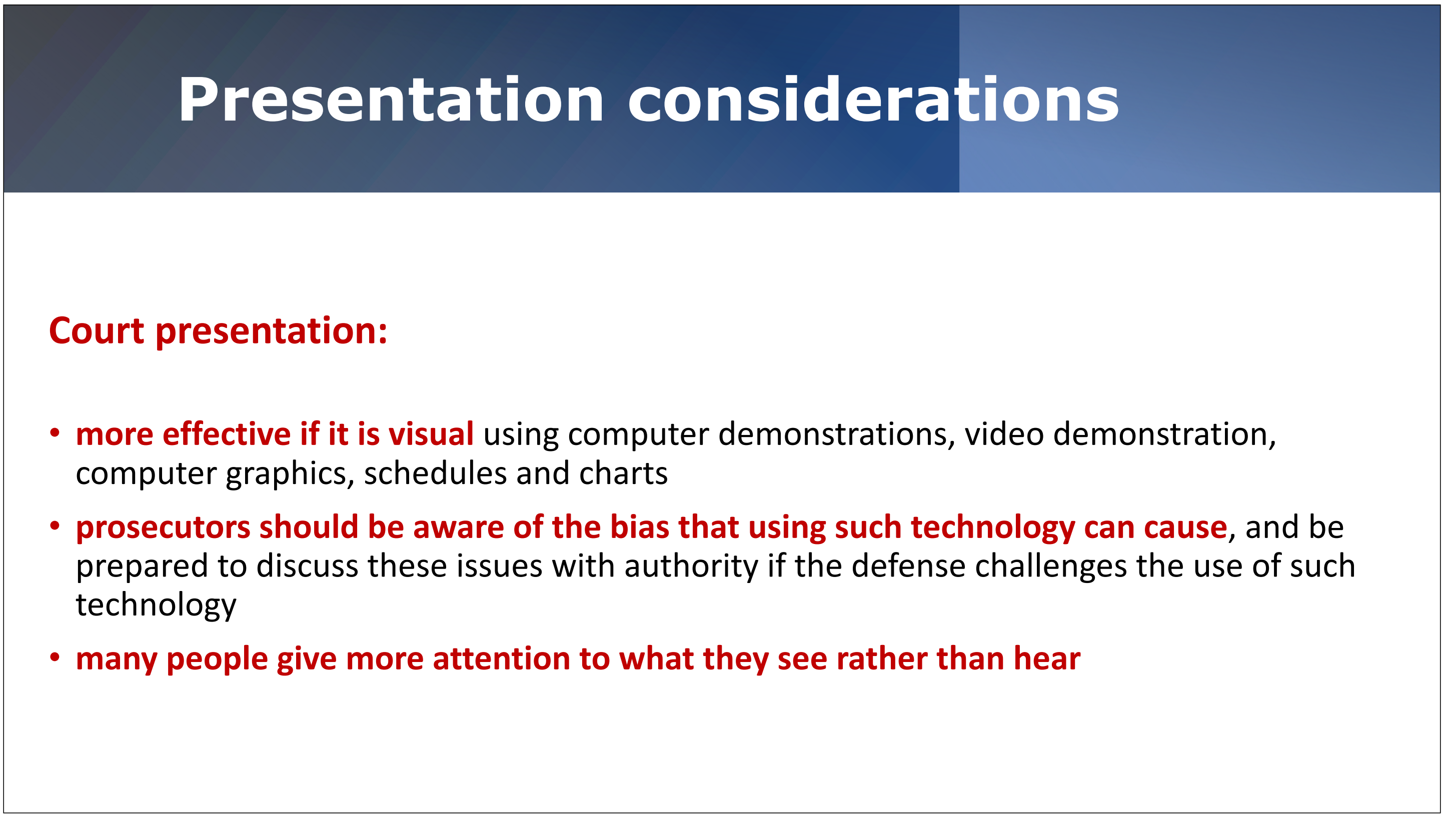
**At trial it is essential to display objectivity**, as well as the continuity and integrity of evidence

**It is also necessary to demonstrate how evidence has been recovered**, showing each process through which, the evidence was obtained

# Presentation considerations

**Disclosure:**

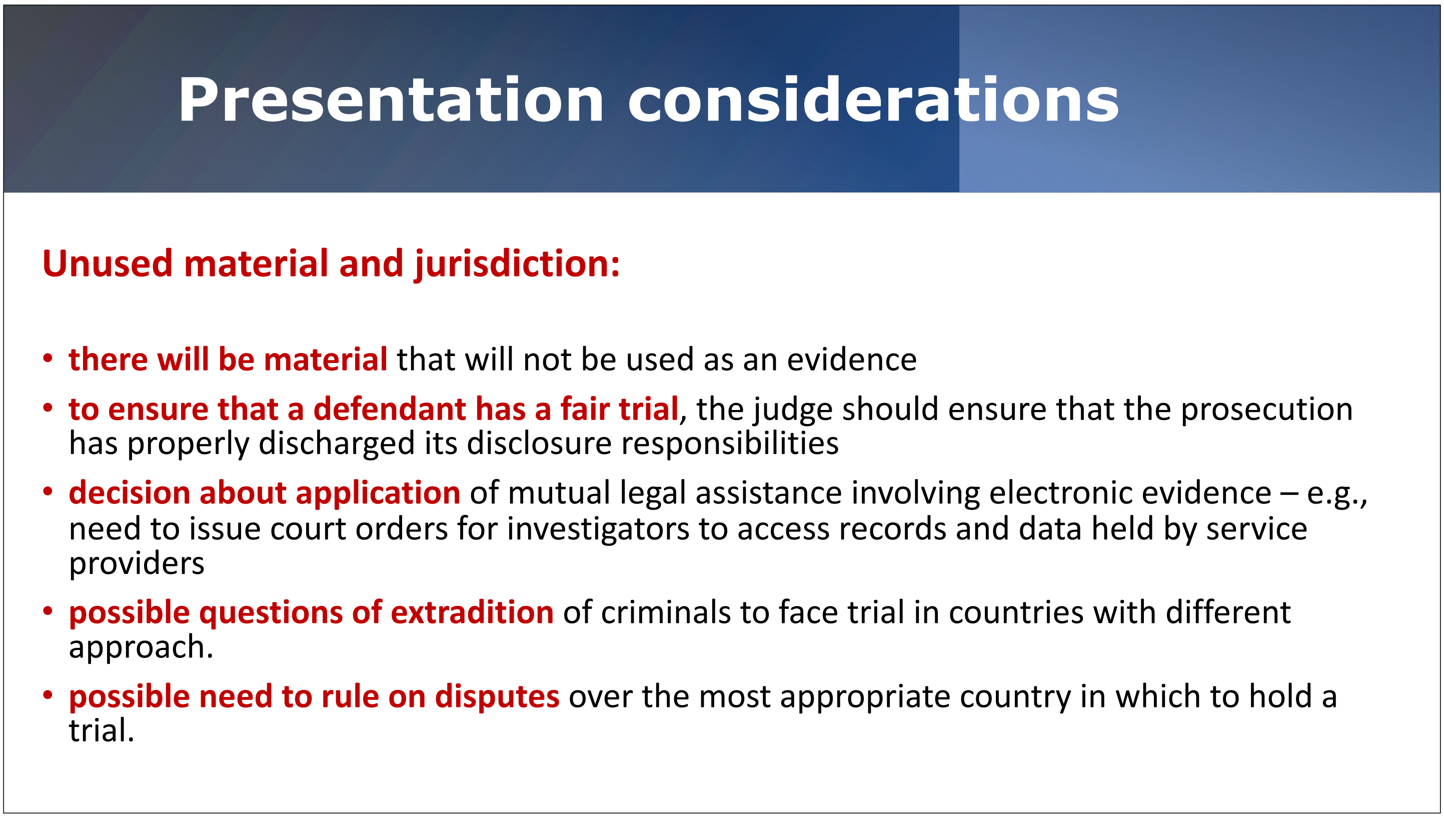
- **each jurisdiction has different rules** and procedures for disclosing evidence to the defense
- **breach of procedure** if electronic evidence is not available for disclosure to the defense
- **evidence should always be accompanied by a full audit trail**



# Presentation considerations

## Court presentation:

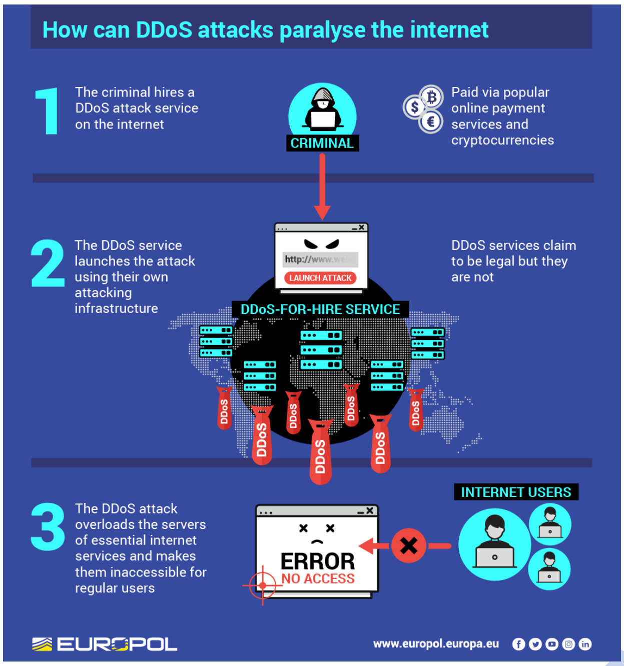
- **more effective if it is visual** using computer demonstrations, video demonstration, computer graphics, schedules and charts
- **prosecutors should be aware of the bias that using such technology can cause**, and be prepared to discuss these issues with authority if the defense challenges the use of such technology
- **many people give more attention to what they see rather than hear**



# Presentation considerations

## Unused material and jurisdiction:

- **there will be material** that will not be used as an evidence
- **to ensure that a defendant has a fair trial**, the judge should ensure that the prosecution has properly discharged its disclosure responsibilities
- **decision about application** of mutual legal assistance involving electronic evidence – e.g., need to issue court orders for investigators to access records and data held by service providers
- **possible questions of extradition** of criminals to face trial in countries with different approach.
- **possible need to rule on disputes** over the most appropriate country in which to hold a trial.



## How can DDoS attacks paralyse the internet

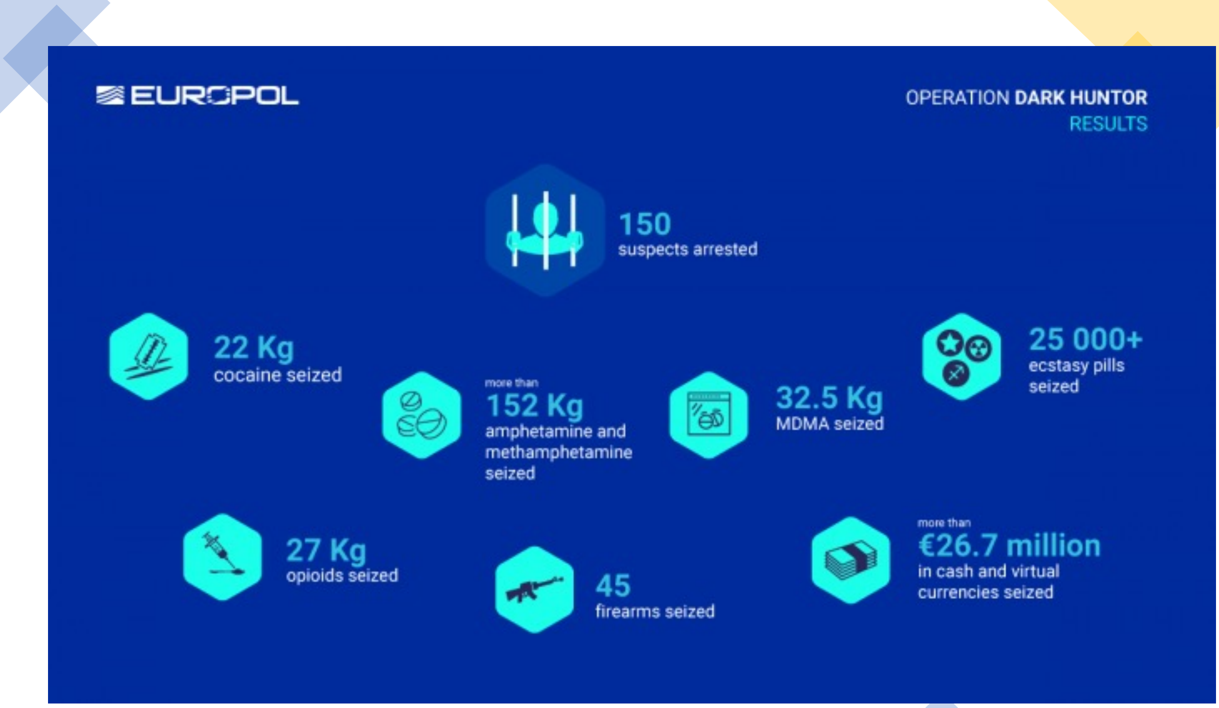
1 The criminal hires a DDoS attack service on the internet

Paid via popular online payment services and cryptocurrencies

2 The DDoS service launches the attack using their own attacking infrastructure

DDoS services claim to be legal but they are not

3 The DDoS attack overloads the servers of essential internet services and makes them inaccessible for regular users



## OPERATION DARK HUNTOR RESULTS

150 suspects arrested

22 Kg cocaine seized

more than 152 Kg amphetamine and methamphetamine seized

32.5 Kg MDMA seized

25 000+ ecstasy pills seized

27 Kg opioids seized

45 firearms seized

more than €26.7 million in cash and virtual currencies seized

РЕПУБЛИКА СРБИЈА
РЕПУБЛИЧКО ЈАВНО ТУЖИЛАШТВО
PTVTK
POSEBNO TUŽILAŠTVO ZA VTK

## ➢ Belgrad Wolfjäger

- **Planned actions by Special Prosecution for Cybercrime of Serbia**:
- **Field-check** of reliability of all data regarding housing addresses of all natural and legal persons connected with criminal activities;
- **Inclusion** of Financial Investigation Unit of MoI and Directorate for Prevention of Money Laundry of MoF;
- **Drafting of all necessary** Search and Seizure Orders, Arrest Warrants, Criminal Investigation and Financial Investigation Orders, together with other Court related documents, is already underway;

РЕПУБЛИКА СРБИЈА
РЕПУБЛИЧКО ЈАВНО ТУЖИЛАШТВО
PTVTK
POSEBNO TUŽILAŠTVO ZA VTK

## ➢ Belgrad Wolfjäger

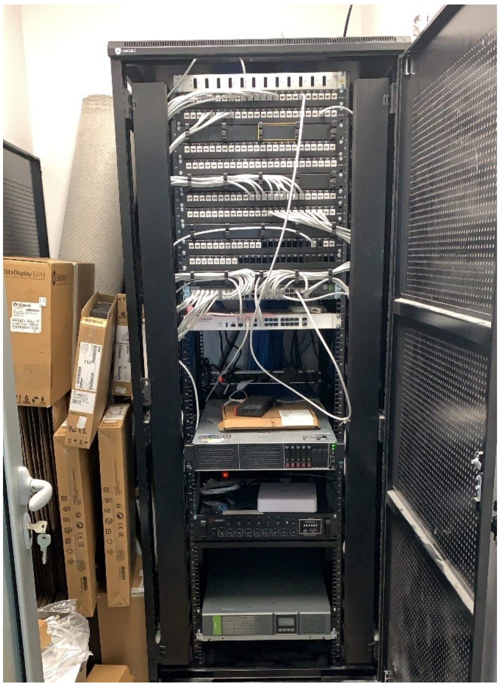
- **National Bank** of Serbia communication and orders for identification of all persons entitled as targeted and connected bank accounts holders or transaction handlers or holders of any other right for managing in any way of the targeted accounts, is under way;
- **Re-checking with German and Austrian counterparts** about missing documents regarding certain persons and targets;
- **Acquiring from German and Austrian counterpart's** victim statements and further evidence about financial damages and money flow;

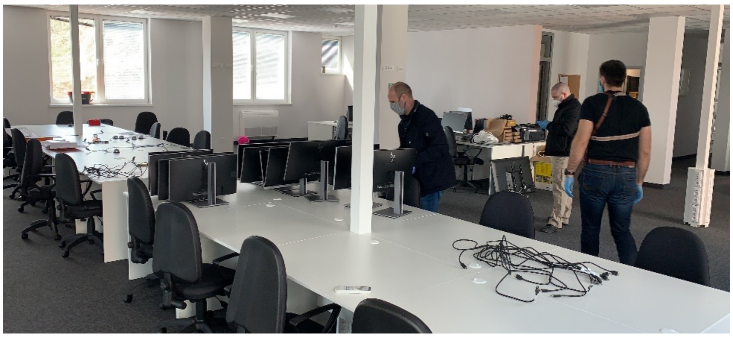
## ➢ Belgrad Wolfjäger

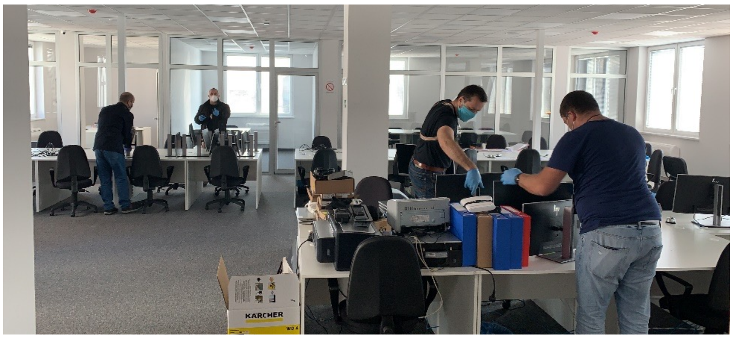
- **Establishing connections** with other International counterparts regarding this case;
- **Agreement** about mutually acceptable date for Action Day;
- **Technical and logistical preparations** for Action Day, including engagement and allocation of additional Ministry of Interior, Ministry of Finance and Public Prosecution resources;
- **Agreement** about possible presence of International partners representatives;
- Other issues;

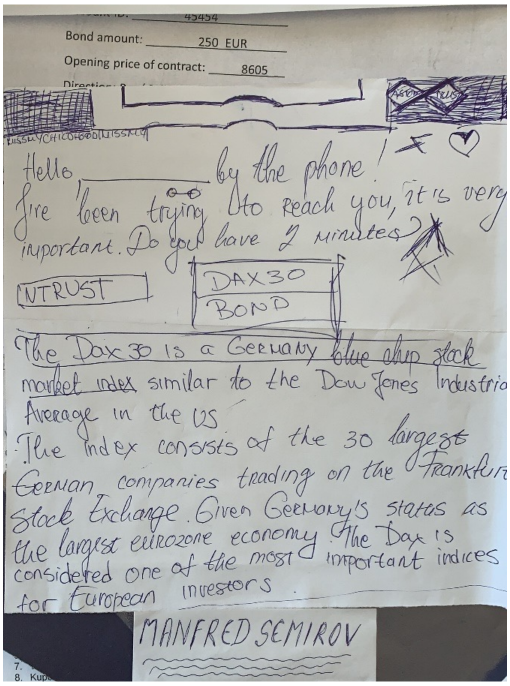
РЕПУБЛИКА СРБИЈА
РЕПУБЛИЧКО ЈАВНО ТУЖИЛАШТВО

PTVTK
POSEBNO TUŽILAŠTVO ZA VTK









Account ID: 45454

Bond amount: 250 EUR

Opening price of contract: 8605

Direction: B

KISSMYCHICOHOODKISSMY

Hello, ________ by the phone!
Jire been trying to reach you, it's very important. Do you have 2 minutes?

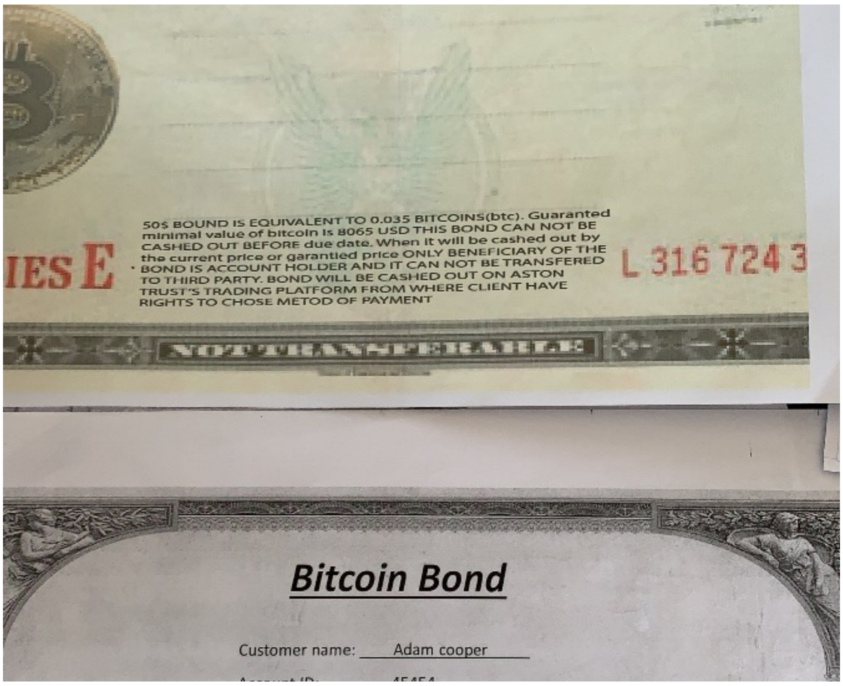
NTRUST

DAX30
BOND

The Dax 30 is a Germany blue chip stock market index similar to the Dow Jones Industria Average in the US
The index consists of the 30 largest German companies trading on the Frankfurt Stock Exchange. Given Germany's status as the largest eurozone economy. The Dax is considered one of the most important indices for European investors

MANFRED SEMIROV

7.
8. Kup



IES E

50$ BOUND IS EQUIVALENT TO 0.035 BITCOINS(btc). Guaranted minimal value of bitcoin is 8065 USD THIS BOND CAN NOT BE CASHED OUT BEFORE due date. When it will be cashed out by the current price or garantied price ONLY BENEFICIARY OF THE BOND IS ACCOUNT HOLDER AND IT CAN NOT BE TRANSFERED TO THIRD PARTY. BOND WILL BE CASHED OUT ON ASTON TRUST'S TRADING PLATFORM FROM WHERE CLIENT HAVE RIGHTS TO CHOSE METOD OF PAYMENT

L 316 724 3

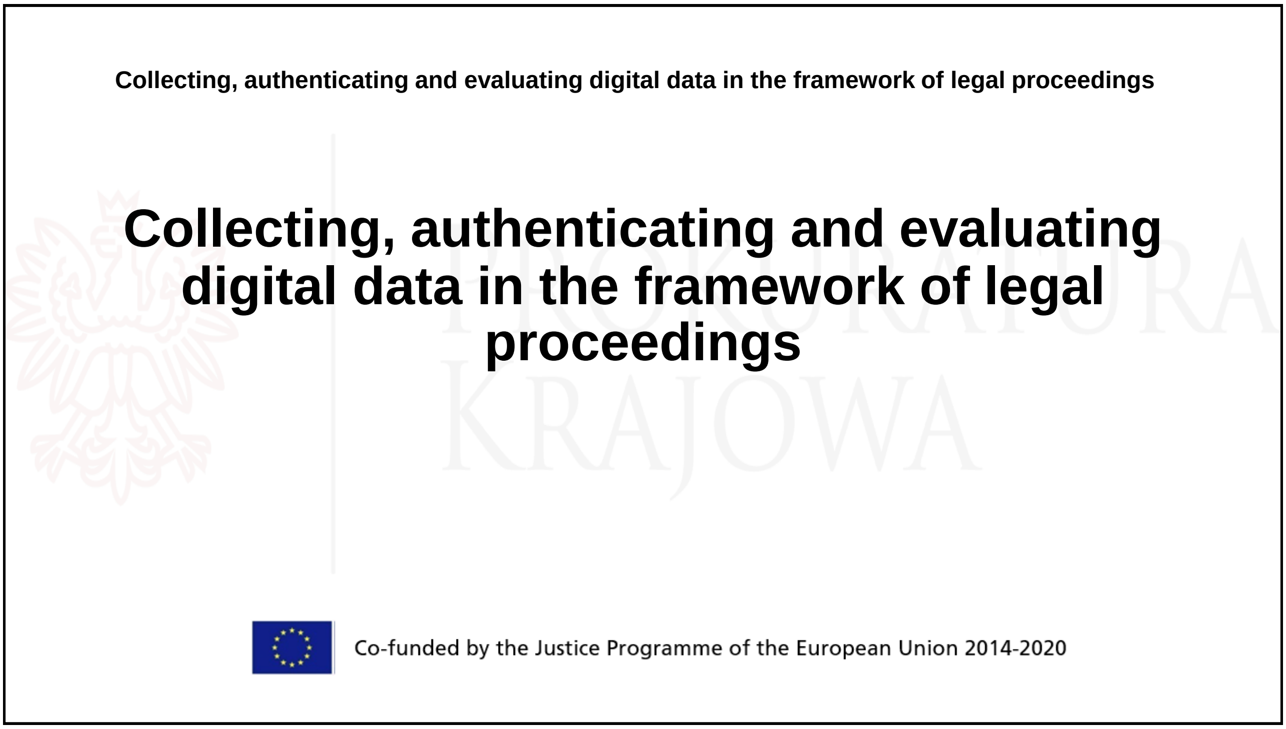
NOT TRANSFERABLE

## Bitcoin Bond

Customer name: Adam cooper

Account ID: 45454

# Thank you

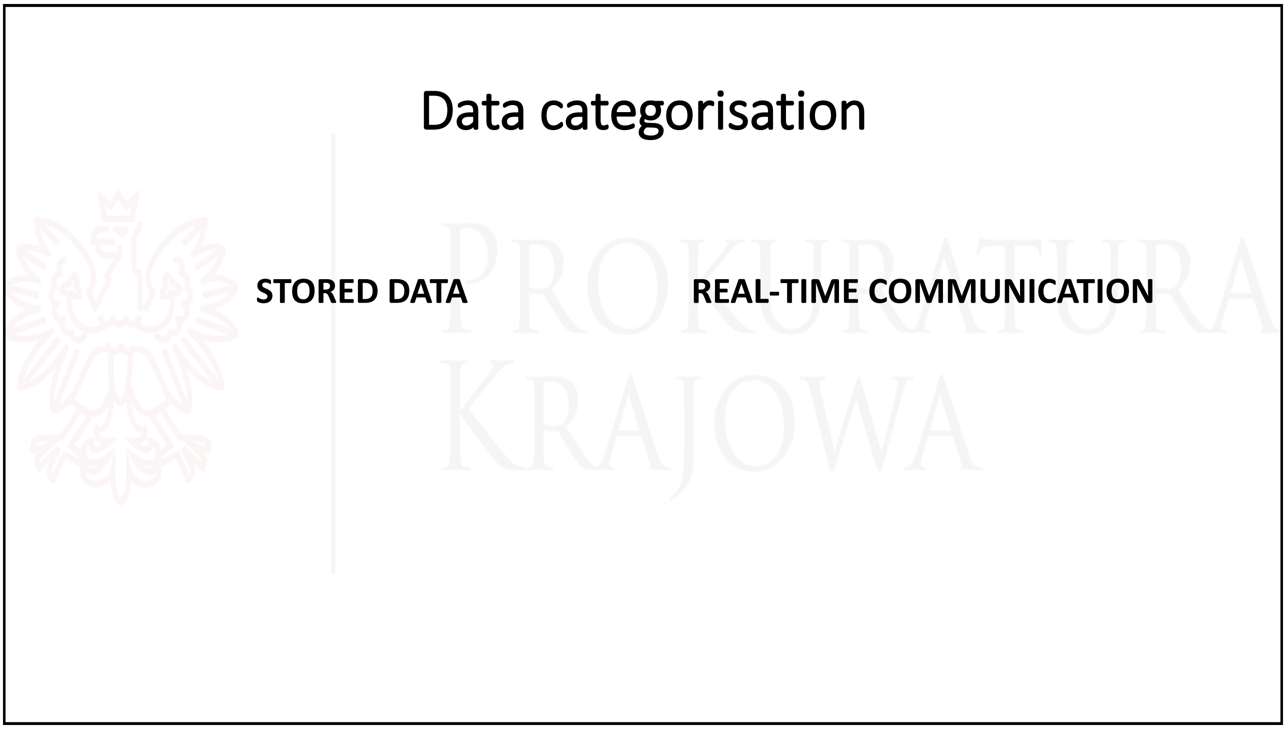


Collecting, authenticating and evaluating digital data in the framework of legal proceedings

# Collecting, authenticating and evaluating digital data in the framework of legal proceedings

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

1



## Data categorisation

**STORED DATA**

**REAL-TIME COMMUNICATION**

2

## STORED DATA

**NON-CONTENT DATA**

**BASIC SUBSCRIBER INFORMATION**

3

## STORED DATA

**NON-CONTENT DATA**

**TRAFFIC DATA**

4

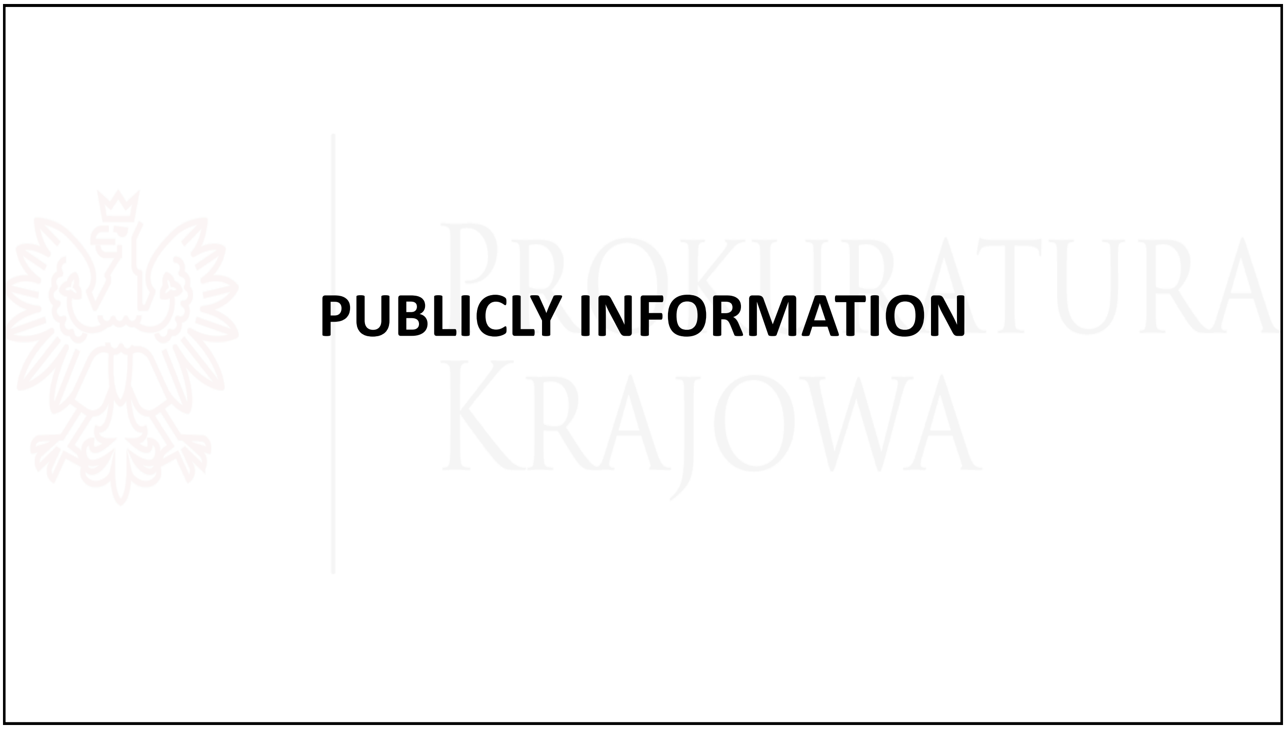
## STORED DATA

**CONTENT DATA**

5

## REAL-TIME COMMUNICATIONS

6



## PUBLICLY INFORMATION

7

## NON-PUBLICLY AVAILABLE INFORMATION

8

# DIRECT ACCESS TO ELECTRONIC INFORMATION

9

# COERCIVE MEASURES

## REAL-TIME COMPUTER AND NETWORK SURVEILLANCE

10

# SEARCH AND SEIZURE OF STORED COMPUTER DATA

11

# FORENSIC ANALYSIS OF STORED COMPUTER DATA

12

## INFORMATION PROVIDED BY PARTIES

13

## DIRECT REQUEST

## VOLUNTARY COOPERATION

14

## DIRECT REQUEST

15

JUDICIAL ASSISTANCE

## PRESERVATION ORDER UNDER JUDICAL COOPERATION

16

JUDICIAL ASSISTANCE

## EURPEAN INVESTIGATION ORDER

17

JUDICIAL ASSISTANCE

## MUTAL LEGAL ASSISTANCE REQUEST

18

# TECHNICAL STANDARDS ON GATHERING ON ELECTRONIC DATA

19

## *SIRIUS*

***PROJECT***

***Knowledge, expertise, experience…its mayby solution***

20

# Thank you for your attention

Tomasz Iwanowski

tomasz.iwanowski@prokuratura.gov.pl

21