european.law

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

From the issuing order to the presentation in court passing by the custody chain

Online Seminar, 8-9 March 2021 (CET)

UP GRADE YOUR LEGAL EXPERTISE

Criminal Law

Professional Training (CPD) www.era.int

Speakers

John Berry, Barrister, Bar of Ireland, Dublin

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

Klaus Hoffmann, Senior Prosecutor Prosecutor's Office, Freiburg

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

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

Chatrine Rudström, Senior Public Prosecutor, Prosecutor's Office, Stockholm; Member of the European Judicial Cybercrime Network (EJCN), The Hague

David Silva Ramalho, Defence Lawyer, Morais Leitão, Galvão Teles, Soares da Silva & Associados, Lisbon

Danijel Sladović, Digital Forensic Consultant, INsig2, Zagreb

Stanisław Tosza, Associate Professor of Compliance and Law Enforcement, University of Luxembourg

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
- Conducting a criminal investigation across state borders: search orders, search and seizure, destruction of evidence, evidence from other jurisdictions, trial
- Chain of custody (through case studies)

Language
English

Event number
321DT32e

Organisers
ERA (Laviero Buono) in cooperation with The Bar of Ireland

THE BAR OF IRELAND
The Law Library

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

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

Monday, 8 March 2021

09:00 Connecting to the videoconference platform and getting familiar with it

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

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

Chair: Laviero Buono

09:35 **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

10:45 Discussion

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

Danijel Sladović

11:45 Discussion

12:00 Short break

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

12:15 **Online investigations and the challenges of dealing with electronic evidence in criminal proceedings**
- Principles of dealing with electronic evidence
- Common procedures for recognising and handling evidence on digital devices
- International investigations (search and seizure – obtaining evidence from the Internet, admissibility)

Klaus Hoffmann

13:00 Discussion

13:15 Lunch break

14:15 **The collection of evidence located abroad and the challenges of cross border access to data**
- Cross-border access to data
- Cloud computing
- European enforcement challenges in the online context
- Shortcomings and remedies

Stanisław Tosza

15:00 Discussion

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 online 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).

Interactive online seminar

The online seminar will be hosted on ERA's own online platform. You will be able to interact immediately and directly with our top-level speakers and other participants. We will make the most of the technical tools available to deliver an intensive, interactive experience. As the platform is hosted on our own server, the highest security settings will be applied to ensure that you can participate safely in this high-quality online conference.

CPD

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

15:15 End of the first day

Tuesday, 9 March 2021

09:15 Connecting to the videoconference platform

09:30 **The European Investigation Order (EIO) and its effectiveness in collecting evidence located abroad**
- Legal framework and problems regarding traditional mutual legal assistance (MLA) in the digital age
- The EIO in the online context
- Specificities and challenges of criminal cases where anonymous networks and encrypted files are involved

Joachim Meese

10:15 Discussion

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

10:30 **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

11:15 Discussion

11:30 Short break

11:45 **Handling electronic evidence in courts**
- The importance of the chain of custody in handling evidence
- Trial considerations: methods of presentation and admissibility tests

Chatrine Rudström

12:30 Discussion

12:45 **Collecting, authenticating and evaluating digital data in the framework of legal proceedings: best practices**
- Issuing order
- Presentation in Court
- Admissibility of e-evidence
- Case studies

John Berry

13:15 Discussion

13:30 End of online seminar

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

Times indicated are CET (Central European Time)

Your contact persons

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

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

Save the date

Annual Conference on White-Collar Crime in the EU 2021
Online, 18-19 March 2021

Anti-Money Laundering for the Judiciary and Law Enforcement
Online/Trier, 29-30 April 2021

Artificial Intelligence (AI) and the Criminal Justice System
Warsaw, 17-18 June 2021

Summer Course on European Criminal Justice
Webinar, 21-25 June 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/?130412&en

Join the Friends of ERA — a Europe-wide network

Friends of ERA Association
Metzer Allee 4
D-54295 Trier

As a participant at ERA conferences and courses you are cordially invited to join the Friends of ERA Association*.
The Friends of ERA also actively supports ERA's work, most notably by providing funding for the ERA scholarship programme to enable legal practitioners who cannot afford the costs to attend ERA events.

MEMBERSHIP APPLICATION

Please select your category of membership

❑ **Annual membership for individuals: € 75**

❑ **Annual membership for organisations: € 1000**

Please enter your name and address information using block capitals or staple your business card:

Title ❑ Ms ❑ Mr Other _____

First Name _____

Surname _____

Organisation _____

Department _____ Tel. _____

E-Mail _____

Street _____

Postcode/City _____ Country _____

Preferred language: ❑ English ❑ French ❑ German

❑ **Annual subscription to ERA Forum at a preferential price of € 95**

❑ I wish to make a donation to the ERA Jubilee Fund

Single donation of: € 50 ☐ € 100 ☐ € 200 ☐ € 500 ☐ € 1000 ☐ € (other) _____ ☐

to support: Scholarships ☐ Training projects ☐ Internships ☐ All these purposes ☐

Method of payment (for regular membership or donation)

☐ Credit card — For credit card payment please go to our website: www.era-comm.eu/friends_of_ERA/join.html

☐ Bank transfer — I will transfer the membership fee to the Friends of ERA's account at:
Sparkasse Trier (Theodor-Heuss-Allee 1, 54292 Trier, Germany)
IBAN: DE 03 5855 0130 0000 9653 76 and SWIFT-BIC: TRISDE55

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

Join the Friends of ERA:

Membership of the Friends of ERA offers you the chance not only to support ERA's work but to be part of a network of like-minded individuals and organisations across Europe committed to the better practice of European law – a network that exists both online and in person.

To find out more, please visit www.friends-of-era.eu

Your benefits from the membership in 2021:

- Exclusive access to online conference documentation on the ERA website
- Annual subscription to ERA Forum at a preferential price of € 95 (normal price € 209)
- Regular networking opportunities with colleagues from the European legal community
- Exclusive invitation to our Chapter meetings
- Access to Members Directory

www.friends-of-era.eu

Tax deductibility: Your membership fee for the Friends of ERA, which is registered as a public-benefit association in Germany, is eligible for the relevant tax incentives for charitable donations if you are based in Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Ireland, Lithuania, Luxembourg, the Netherlands, Poland, Slovenia or the UK. In addition, donors based in France, Hungary, Italy, Romania or Switzerland can take advantage of the Transnational Giving Europe network (www.transnationalgiving.eu) to make their donations tax-efficient.

Place, Date _____ Signature _____

Electronic Evidence

Seminar at the Academy of European Law
8-9 March 2021

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

Klaus Hoffmann, Senior Prosecutor, Freiburg

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

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

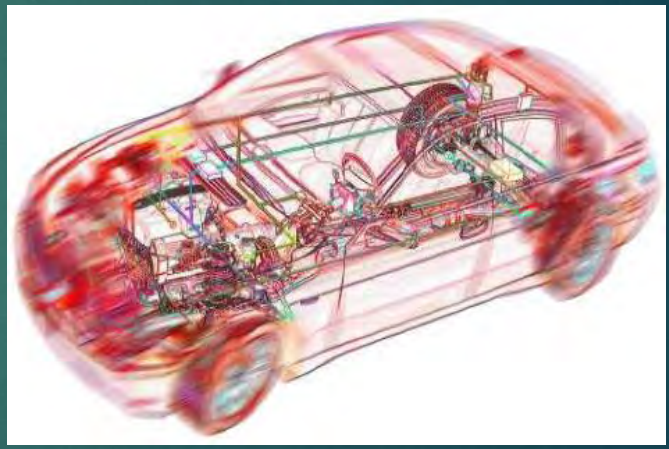
quick introduction

- different kinds of electronic evidence - examples

→ Think of digital devices in your daily life

incl. :

- many SIM cards in moderns cars,
- smart home devices,
- smart phones,
- smart refrigerators,
- washing machine and other electronic / smart devices



Principles of dealing with electronic evidence

- no specific regulations in the (German) Criminal Procedure Code
- various (soft) regulations within different authorities (e.g. police, federal authorities like the German Federal Office for Information Security (BSI))
- best practices and efforts to certificate certain IT forensic software
- general principles of dealing with analogue evidence also apply to digital / electronic evidence

Principles of dealing with electronic evidence

key aspect:

- ensuring authenticity of digital data
- chain of custody
- proper and detailed documentation of access to data, its storage, copying and analysis
- analysis and further work with digital data is only done with a copy, not the original set of data
- proper documentation of the police staff that is involved and the IT forensic software that is being used

How is digital evidence handled in court??

limited categories of evidence

- witness testimony
- expert testimony
- documentary evidence
- evidence by inspection(e.g. photos, videos, tangible objects like a gun)

▶ Digital evidence has to be presented in one of those categories.

How is digital evidence handled in court??

- case examples (WhatsApp messages, child porn files, telecommunication data)
- extra note on IT expert witnesses
- analysis of Bitcoin evidence - extra group of Landeskriminalamt (state police) to collect and analyse bitcoin evidence across many cases

International investigations

- Increased relevance of electronic evidence in criminal investigations
  - increased volume of cross-border requests submitted by EU authorities to OSPs in 2019 with a large majority of them issued by Germany (37.7% of requests), France (17.9%) and the UK (16.4%)
  - requests to access electronic data doubled in Poland and nearly tripled in Finland. Furthermore, emergency disclosure requests increased by nearly half in one year.

International investigations (search and seizure – obtaining evidence from the Internet, admissibility)

- case: Online webshop for selling drugs
- European Investigation Order to seize date in The Netherlands
- here: especially bank data or records of orders of the webshop
- first step: seizure of data according to national law
- second step: transfer – how? digital - by which means or analogue: print out?

International investigations / admissibility

- case law by the German Federal Court: based on the idea of mutual trust – evidence obtained by means of MLA / EIO is in general admissible
- if requirements under German procedural law are fulfilled
- and international cooperation according to law on mutual cooperation has been applied

- how about direct access to online data? →

Proposed EU order

European production and preservation order (EPO)

- relates to specific telecommunication data and social media files
- doesn‘t address the regular access to electronic evidence in other countries
- example: access to digital data seized from a webserver in France or Spain
- controversy discussion at the European Parliament; see e.g.: *review of Stanislaw Tosza in* Eucrim 4/2018

another example: access to Facebook data

- *access to an open account*
- *access to a closed account of a suspect*
  - *invitation to any other user (e.g. "Micky Mouse")?*
  - *restricted access – undercover agent needed?*
- *suspect/ witness opens his account to be used by police*

- *for more details see: Eucrim 3/2012 (p. 137 et seq.)*

Challenges and solutions

- challenges in retrieving relevant data from abroad
  - length of relevant procedures in place
  - language barrier
  - different legal procedures and competences
  - very limited time that data is stored
  - different standards on cooperation by private companies
  - encrypted communication
  - sophisticated means of communication

Challenges and solutions

- Training, knowledge exchange and a centralised approach
  - technical training of judges / lawyers
  - hiring more and better trained staff at the police (and in judiciary)
  - technical equipment in court
  - special point of contacts with private companies
  - GPEN – network of the IAP
  - SIRIUS – exchange platform of Europol

Challenges and solutions

- issues at domestic level
  - similar issues as before
  - technical equipment in court
  - technical training of judicial staff
  - massive volume of data
  - new legal tools to deal with encryption?
  - despite specific rules on electronic evidence – its presentation and admission is mostly not a problem

Questions / Comments?

- For any comments or questions, please feel free to contact me:

Klaus Hoffmann

Staatsanwaltschaft Freiburg

Berliner Allee 1, D-79104 Freiburg

email: klaus.hoffmann@stafreiburg.justiz.bwl.de

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

Scope

What are we talking about here?

How does the Internet work?

Internet vs social media 1.0/2.0

Hidden features 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

Non opensource techniques

All the answers

Case Study

GameStop

The set up

GameStop is one of the last US brick and mortar store franchises selling video game related merchandise.

The stock traditionally was performing at a low price

Wall Street investments firms bet that the stock price was going to be even lower. They '**shorted**' it

Online amateur investment communities, typically made up of young individuals who had a fondness for GameStop, noticed this situation and decided the stock was good investment

Primary promoter is a Reddit user called u\DeepFuckingValue; real name **Keith Gill** but there were other motivators as well

The event

Over a couple of days, the Reddit Wallstreetbets community organized and bought GameStop stocks on mass to raise its value.

It rose to 50 times its original value

The stock rise allowed those who invested early to sell at a large profit

The Wall Street hedge funds who bet that the stock would lose value had to offload their positions and buy more GameStop stock.

This lost them lot of money

This tactic is called a **Short Squeeze** and is well known

The Aftermath

This was one of the first large scale Short Squeezes organized by grass roots investors, also known as 'retail investors' via investment app on mobile phones.

The communities organized via social media: **Reddit, Facebook, Discord, Twitte**r.

They made purchasing GameStop stock 'viral'.

The SEC is doing an investigation to see if fraudulent information was used to boost the value of the stock.

Did real professional investors use social media and capitalize on the forum's fervour?

Where do we look for evidence?

Case Study

GameStop saga by the numbers.

How did we identify all this?

How can we collect it?

Reddit

r\WallstreetBets Users

9m

r\Wallstreetbets Posts Per Day

58,157

Facebook

Robinhood Stock Traders Users

161K

Robinhood Stock Traders Posts in February

4,146

Keith Gill

Social Media Accounts

3

Total Followers YouTube and Twitter

710k

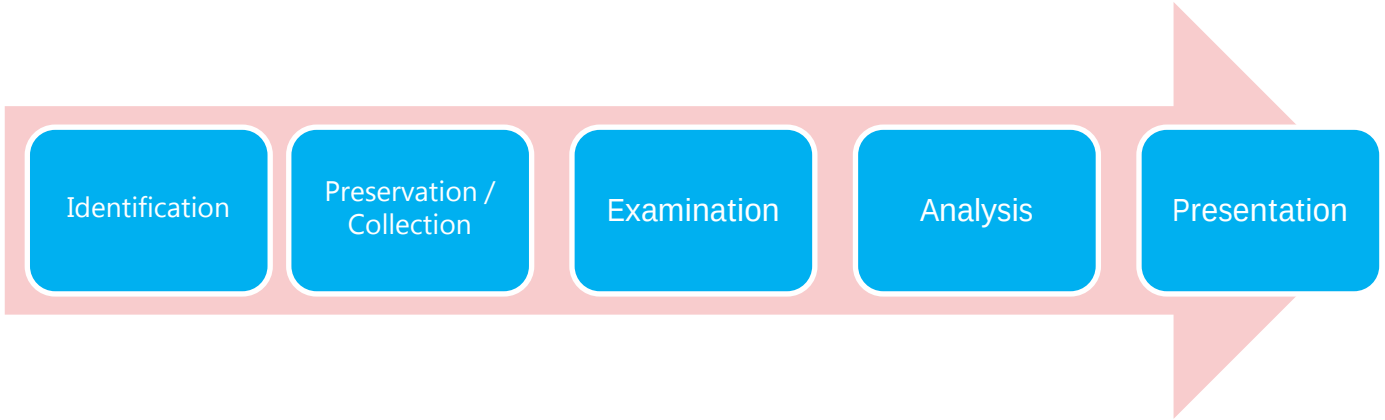
Roaring Kitty YouTube Videos

90

Roaring Kitty Tweets

714

General Forensic Process



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

Internet Basics

The anatomy of the Internet

The internet is a collection of interconnected servers. Each server accepts connections and reverts with information. It ‘serves’ the information back.

Each server is uniquely addressed by IP Addresses

Each IP addressed is resolved to a URL by a DNS.

Components:

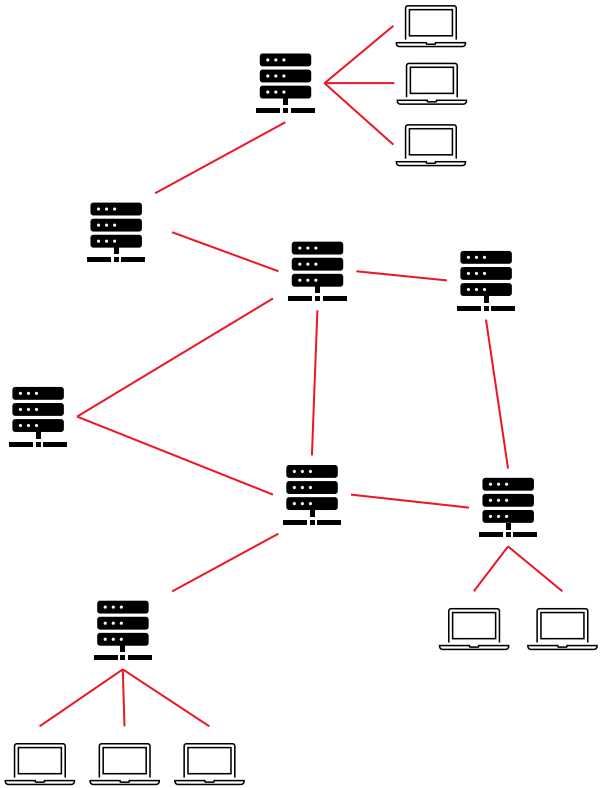
ISP – Internet Service Provider

DNS – Domain Network Service

Packets – individual components of data

World Wide Web – collection of webpages

The Internet is the physical infrastructure, the WWW is built on top of it



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 and some of my photos
- Space is reserved for adverts
- YouTube hosts my videos so rather than hosting it I ‘embed’ it into my page

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

Individual elements of a webpage are stored in a folder

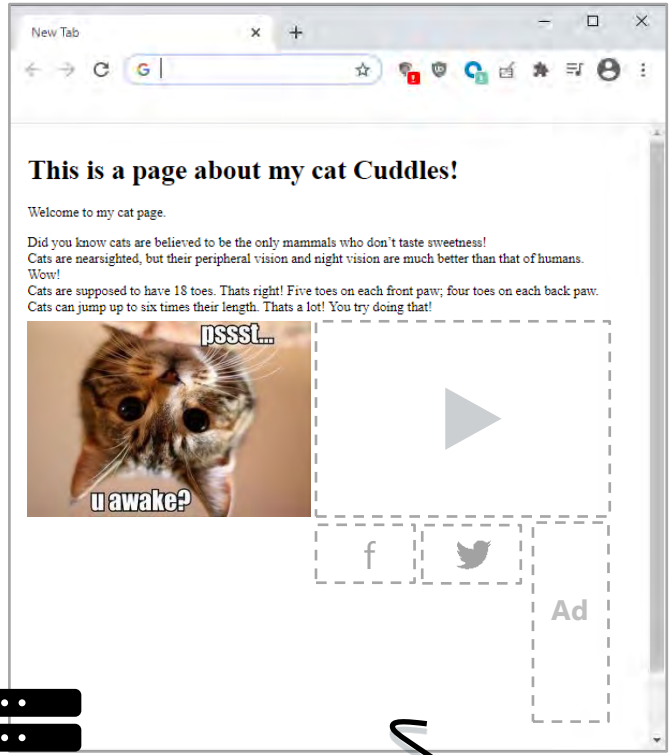
At destination (client side)

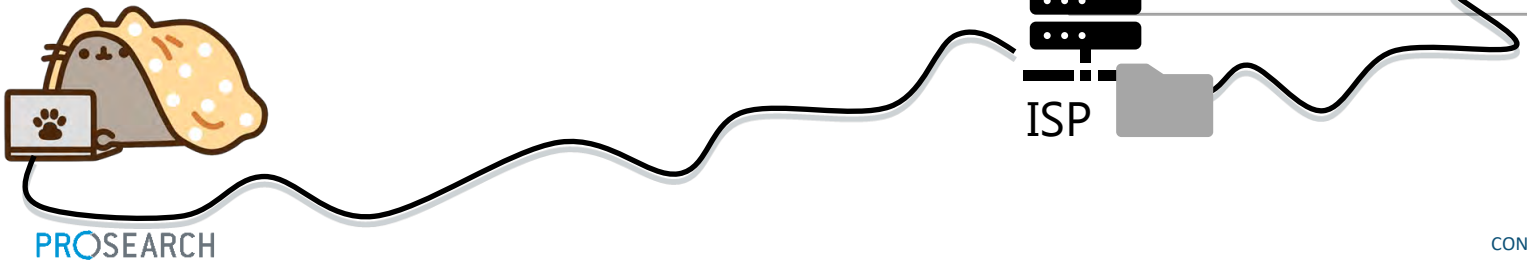
Users log into the webpage

The ISP server sends all elements of the webpage.

‘Embedded’ elements are retrieved from YouTube, Facebook etc.

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





PROSEARCH

The anatomy of a webpage

Individual **Files** making the page

84

Distinct **Domains** the site is connecting to

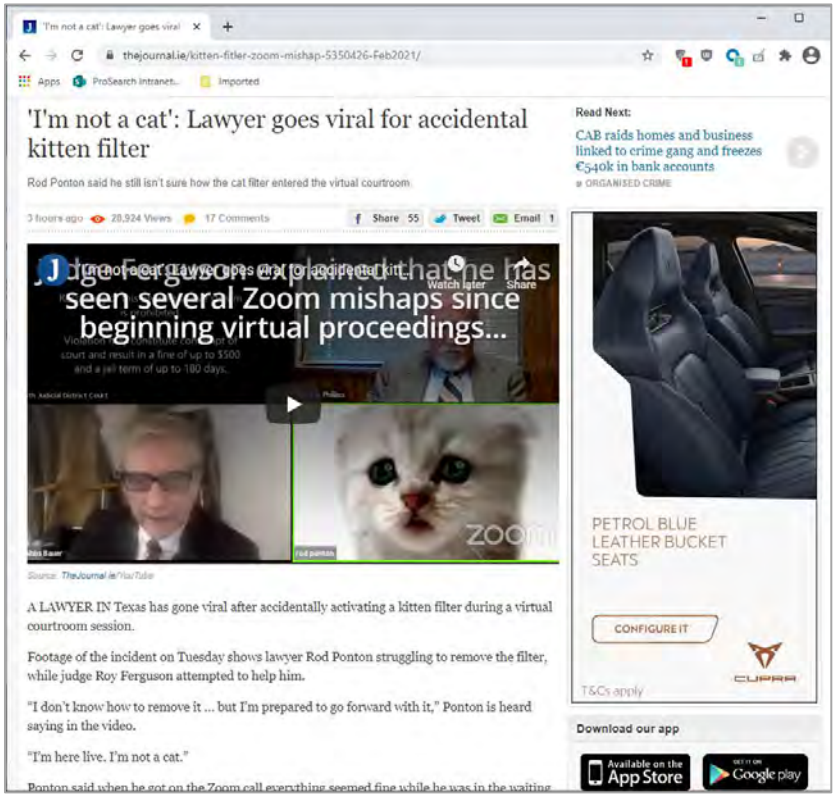
12

Videos downloaded

0

Adverts downloaded

10



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

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 of embedded items

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

Meta tag

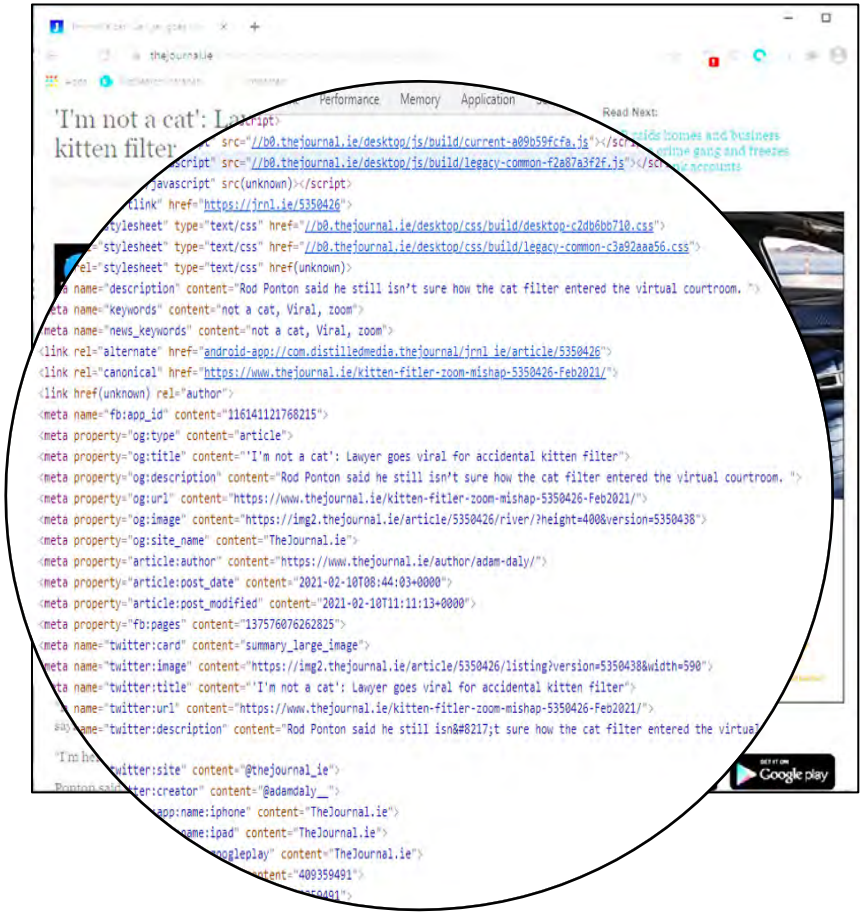
<meta name="article:post_date" content=2021-02-10T08:44:03+000">

Comment tag

<! -- -->

'Hidden' tag

<input type="hidden">



Webpage DNA

JavaScript

Creates dynamic elements of page.

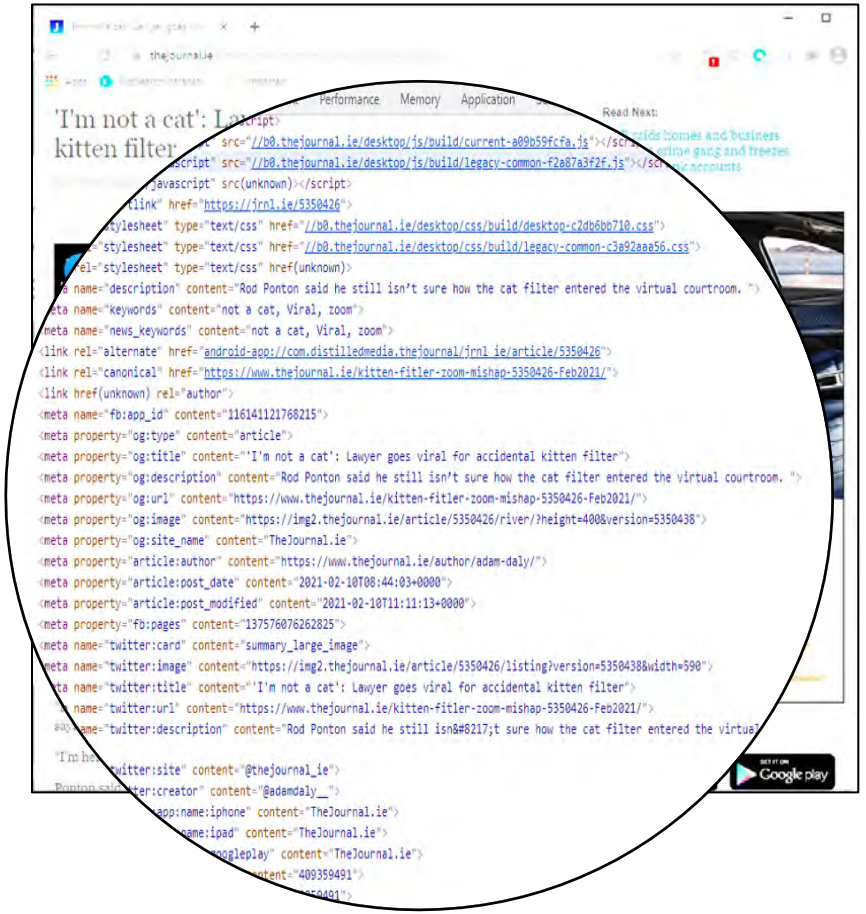
Rather than hard code instruction it runs a small program to show the required data

Changes the ‘client side’ behaviour of the page

Browsers execute the code in the webpage and generate new content

Flash (discontinued)

HTML 5



Web 1.0 v Web 2.0

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

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 have to do is to fill in the blanks

An explosion of personal content:

- Blogs
- vBlogs
- Personal websites

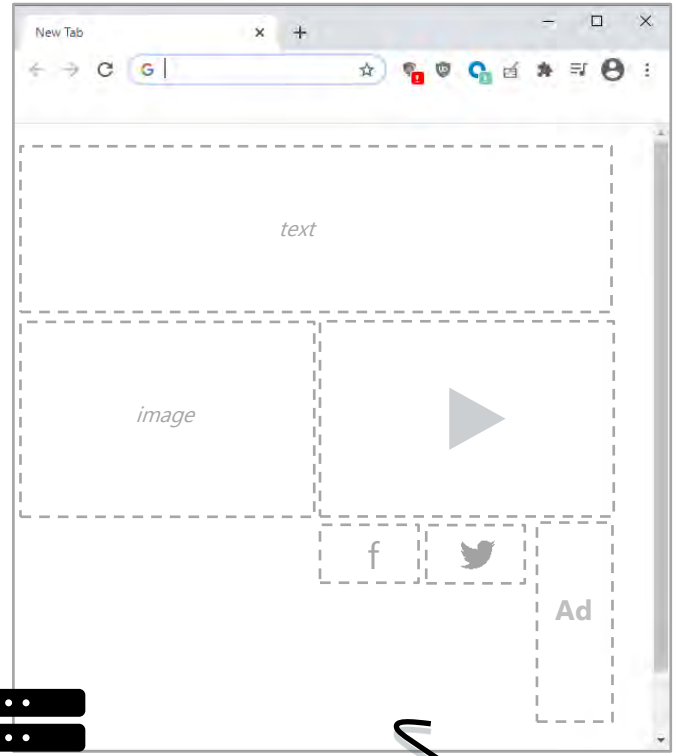
Social Media Sites

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.



PROSEARCH

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 have to do is to fill in the blanks

An explosion of personal content:

- Blogs
- vBlogs
- Personal websites

Social Media Sites

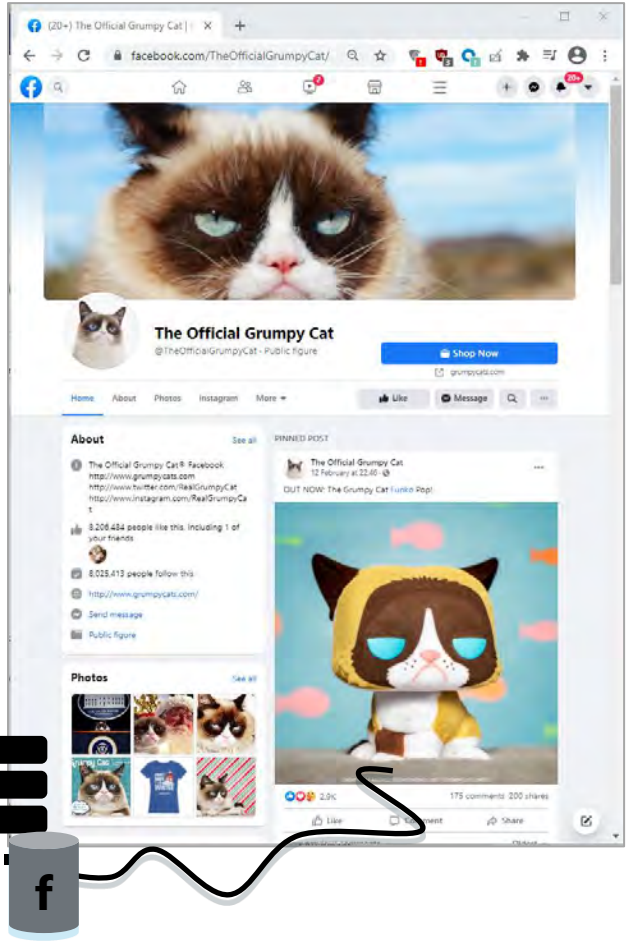
All use some sort of a template to make the page

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.



PROSEARCH

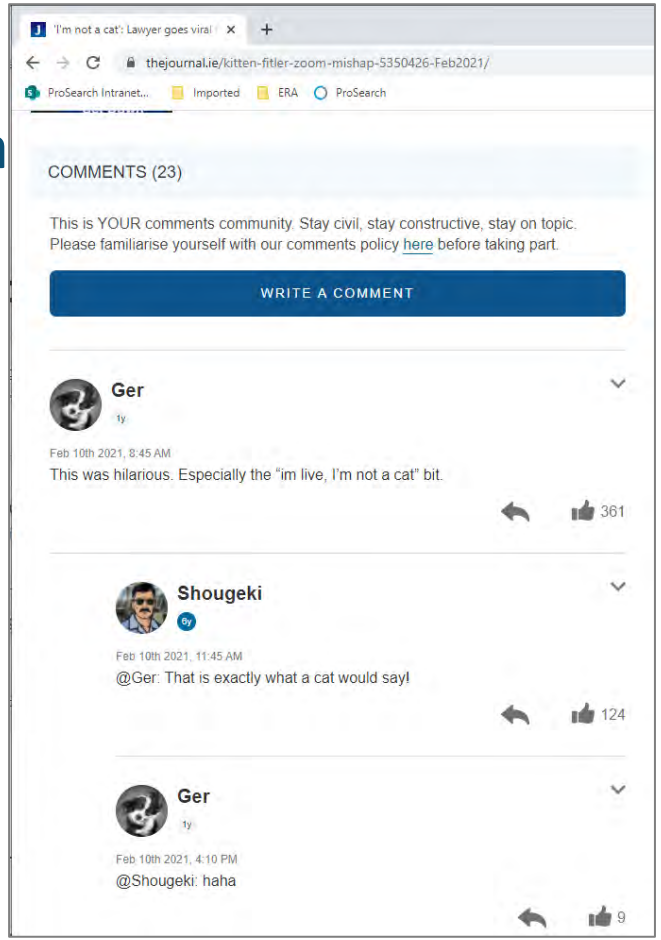
Social Web: More than just Social Media

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’



Hidden Information in a Reddit Post

Reddit webpages

Reddit comments are all found on a single page

That page is **not** fully loaded. Comments are hidden until expanded

Posts can be

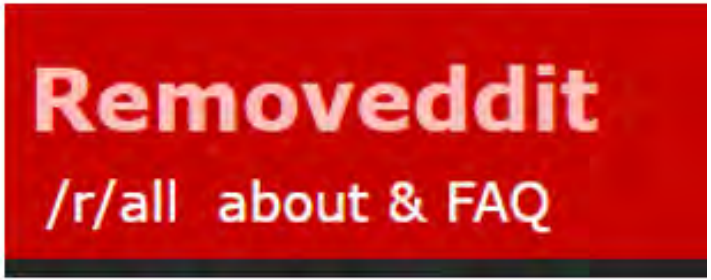
- deleted by the user
- removed by the moderator
- edited by the user

Retrieving Removed Information

Removeddit

Archives deleted and removed Reddit post periodically.

https://www.removeddit.com/



Archive.org

General web archiving service.

May or may not have taken a snapshot of the entire page

General Forums

Boards.ie is a ‘reddit’ of Ireland

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

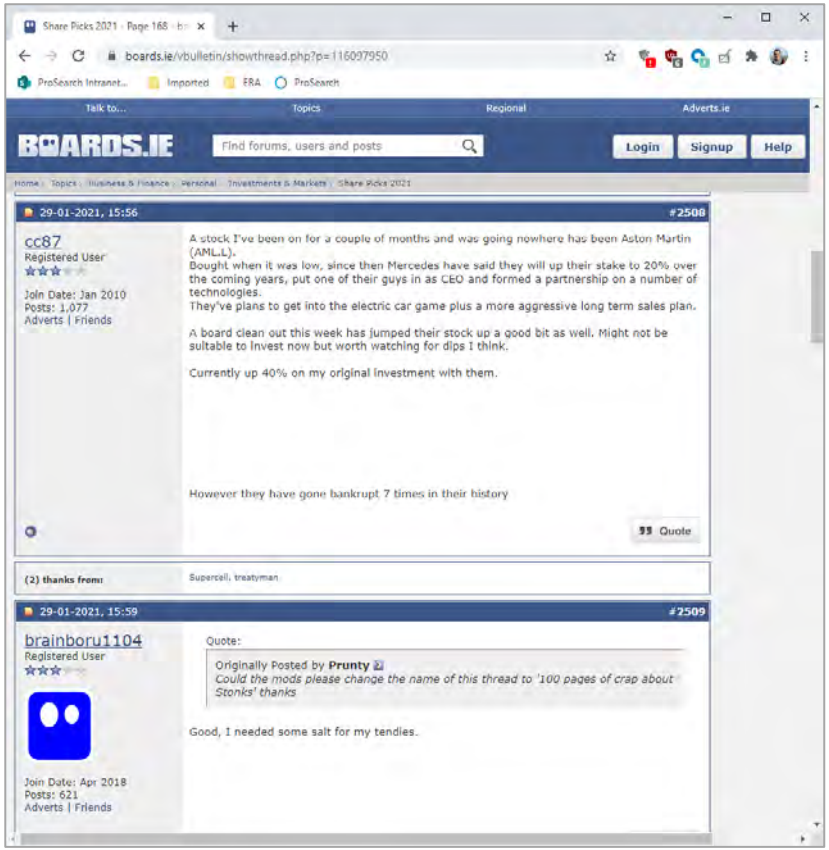
Similar to Reddit

- 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



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%

To Summarise

What do we need to know?

1. A webpage is made up of multiple elements that:
    a) may not be fully known to the user
    b) may be stored in multiple locations
    c) may be dynamic
    d) may not be visible.
2. Web 2.0 sites may keep elements of the pages in databases away from the webpage infrastructure
3. Social Web websites information may be found **strewn across multiple pages** or hidden within a single one. We need to see all of the data to get context.

4. Knowing all that… what are the main ways that data is found?

Internet Searches

Back to Basics

The anatomy of searching

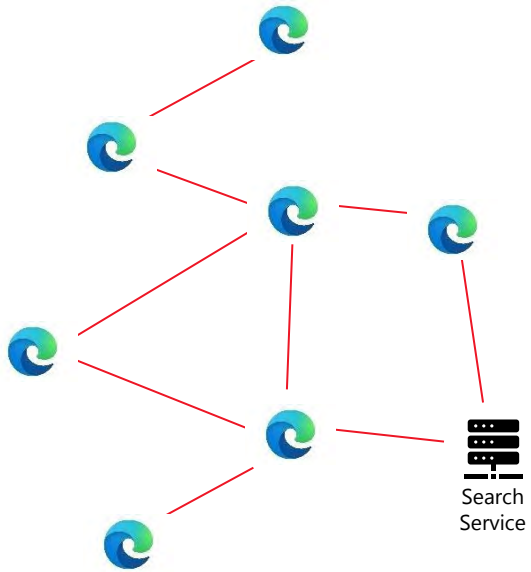
‘Web Spiders’ regularly go from webpage to webpage looking for information. The list of pages they visit is taken information from site maps or from previous crawls

The crawlers follow links on the pages and sends the information back to be organised by the service. The way it is organised depends on how the service works.

The ‘index’ is built from this information.

When searching, users search **this** index, not the live internet.

The quality and completeness of the index defines your results…



What's not in the index?

Surface Web

Everything publicly seen and addressable online

Deep Web

Any data not immediately accessible to the crawler.

Think of services that need you to log in:

- Private mail,
- Social media
- Personal accounts
- Sites where you need to run a query to extract content

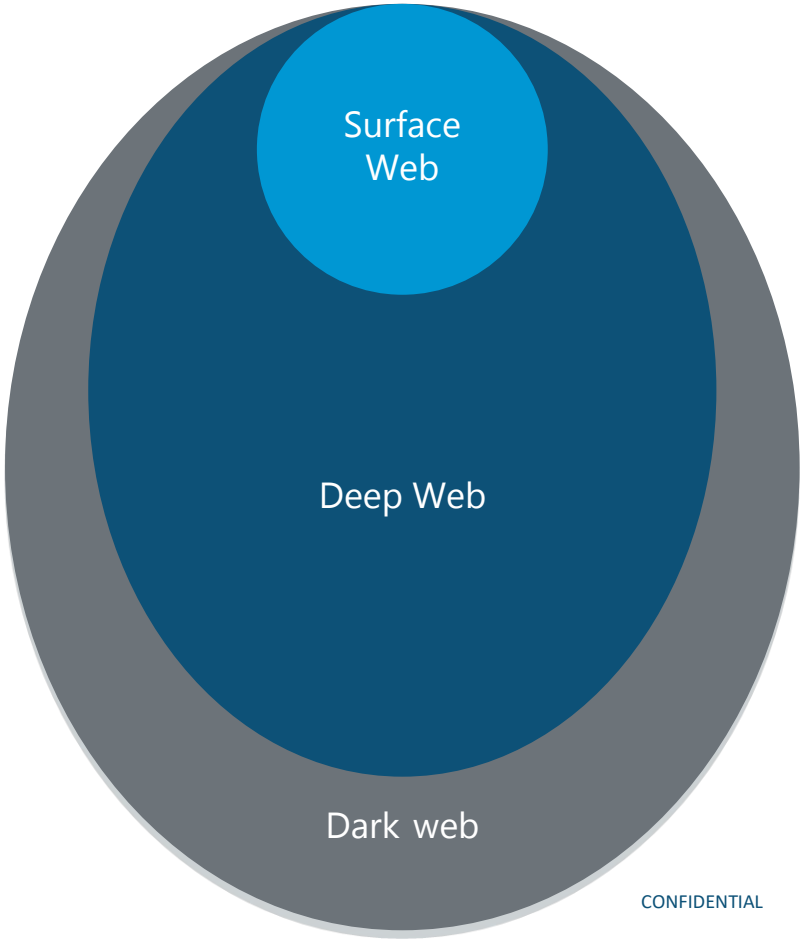
Websites can also limit crawling using robots.txt file, CAPTCHAs,

Dark Web

Can be considered part of the Deep Web but is generally understood to be separate

This stores intentionally hidden information and is generally illegal, Tor etc.

Mainstream search engines ban indexing of illegal material.



Questions?

What are we looking for?

Are we looking for a social media posts or a comment?

Or are we looking for more than that? The entire conversation, the reactions of others, context?

Where do we look for it?

Is the search engine reputable?

How can we look for it?

What features of the search engine are available to us

Some search engines have known limitation.

Their index may not include all the stuff we want to find

Their results may not be displayed in the way we would like

What are we looking for?

Content

- Post, Messages or content that a specific user has put up.
- Metadata showing authorship, time and date of the post
- Exact media
- Proof must be made that the content is not tampered and reliable.
- Metadata hashes should be used to create a signature of the file

Questions:

- What posts \ comments were made in a specific date range?
- What is the context of the post \ message or comments. What is the conversation around this post?
- What were ALL posts \ comments \ messages created by the users

Relationships

- Reactions by other users. Other user's posts influenced by the original poster
- Relationship between the original poster and the community
- Evidence of connections, further social media profiles and social media
- Focused on statistics and understanding the scope of the investigation

Questions:

- How many replies \ messages were made in a specific date range?
- What other web sites were being linked to.
- Are there any other social media sites \ locations that need to be investigated?

Where do we search content?

Reddit Search

Reddit Search

The Reddit site offers a search capability to search the site's content.

Do not need to be logged in or to create an account

Big limitation is that it does not search comments, just posts.

Generic Search Sites

Google \ Bing

Generic search can be tailored to focus on the site in its totality.

Since its all public all information is indexed and searchable

Social Media Specific Search

Social-Searcher.com

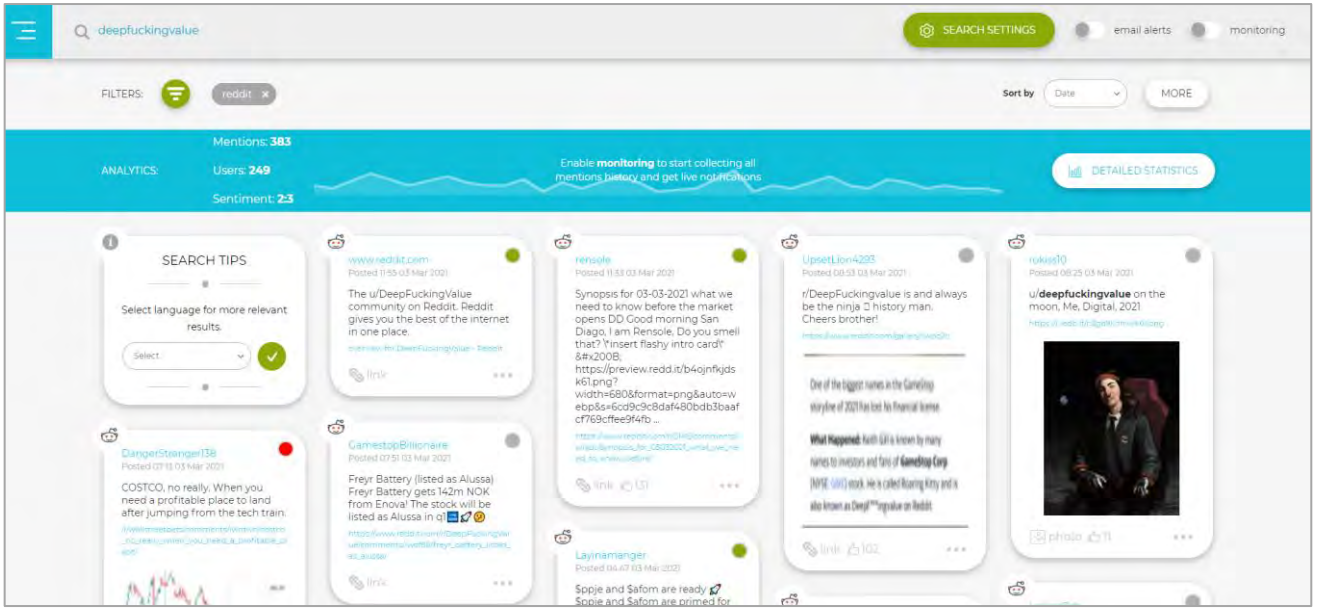
Real time social search.

Supports Twitter, Facebook, Youtube, LinkedIn, **Reddit**, VK, Flickr etc…

Real time monitoring

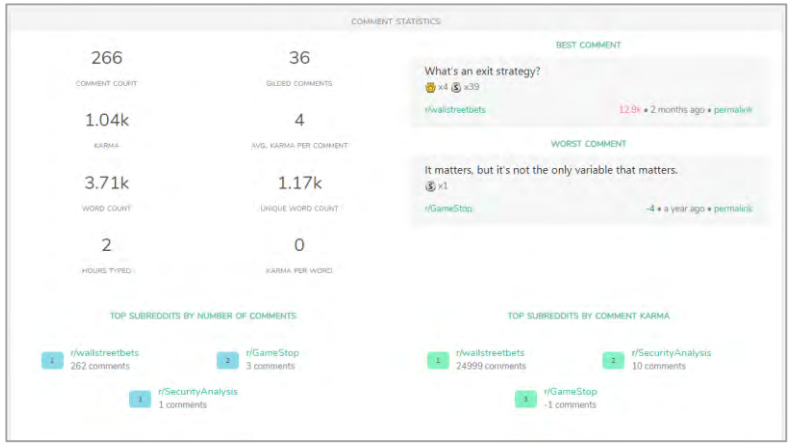
Export of data to CSV

Where do we search content?

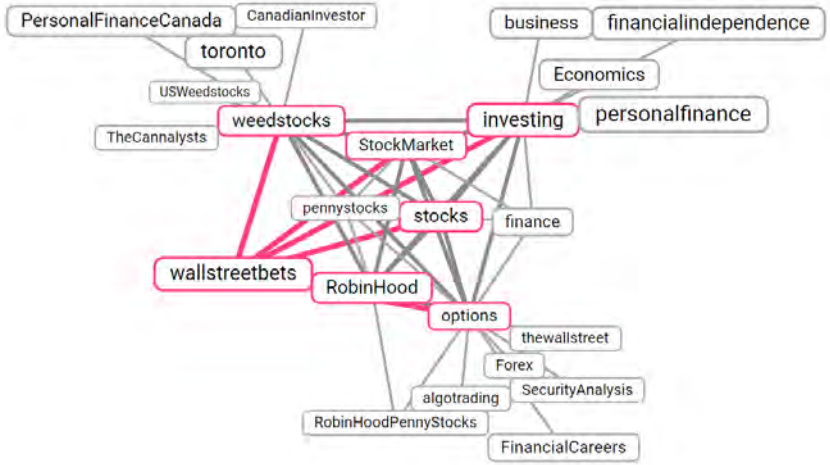


Where do we search relationships?

https://redditmetis.com/



https://anvaka.github.io/sayit



How: Keywords and Terminology

Understand the community

The users typically have their own language, acronyms and ways of speaking

Understanding them allows you to search more effectively.

They may or may not have a glossary of terms to describe language to new members

Wallstreetbets

- **Tendies**: the stocks that the users have bought
- **Paper hands:** investors who sell their stock quickly
- **Diamond hanks**: investors who hold on to their stock even though it may be losing value
- **Stonk**: Another word for stock
- **Rocket ship** (emoji): An expression of the stock rising in value quickly
- **Yolo**: You only live once

How: Basics of Searching

Boolean

AND: apples AND bananas

results must have all the terms

OR: apples OR bananas

results must have at least one terms

NOT: apples NOT bananas

result must have the first but not the second term

PHRASE: “apples and bananas”

result must have the exact phrase

Groupings: (apples AND bananas) NOT pears

group parts of a search together

Concepts

Stemming: identifies the root of the word and expands the search to include all variations

“run” also searches for “running”, runs, ran

Regular Expressions: uses wildcards to create patters to look for, rather than specifying the exact terms to look for

*

?

Sematic (Concept) Search: searches on the meaning of the words, rather than the exact syntax match

Sentiment Analysis

Fields

Depends on what is supported by the search index and provider

How: Fields

Reddit Search

author: The user who submitted the post.

flair: The text of the link flair on the post.

nsfw: Set to yes for NSFW

self: Text post. For example, self:yes or self:1

selftext: For self-posts, the body of the post. selftext:cats

site: The domain of the submitted URL. site:example.com

subreddit: The submission's subreddit. subreddit:cats

title: The submission title. title:cats

url: The submission's URL. url:cats

Google Search

site: Search a specific site

-**site**: Search everything except this site

Cache: Search Google's Cached content

#..#: Search between two years

Related: Find any content related to this site

AROUND(X): Proximity search

Considerations

Problems of Online Search Engines

They focus on finding a single comment \ post or tweet with the appropriate keywords. We are interested in all of the replies, interactions and offshoots of that conversation

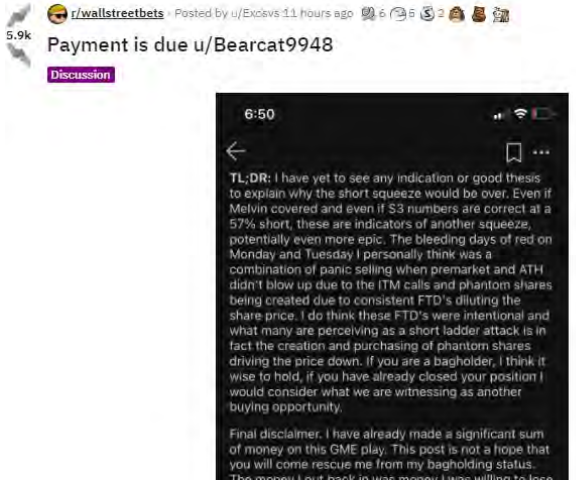
Limited Search capability. We would like to do a search to gather all post created within a certain date range by certain users. Currently not possible.

Many of the posts contain **images** with text. Traditional search engines are not able to OCR the image.

Complex queries combining sentiment analysis, with language identification and regular expressions are not possible

Ultimately, its an uncontrolled environment. Are you getting everything that you want to see? Search engines have limitations and may not present a full picture.

Forensic tools usually have their own indexing engines. We first collect the data, index it ourselves and then run our investigation.



Internet Collections

Collection Aims

ACPO Guidelines

Knowing what we know, can ACPO guidelines be applied to online data?

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

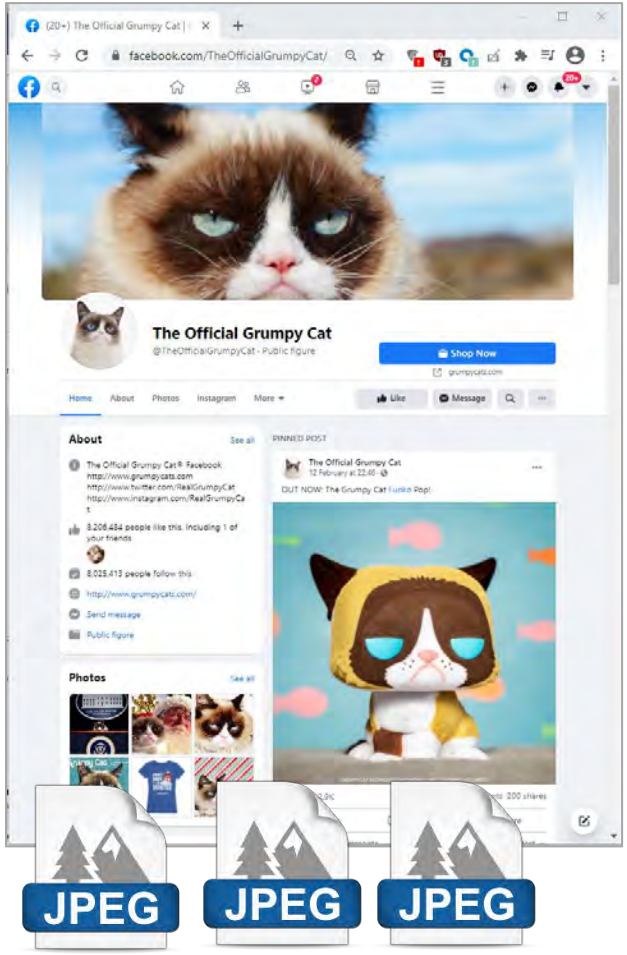
Screenshot

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



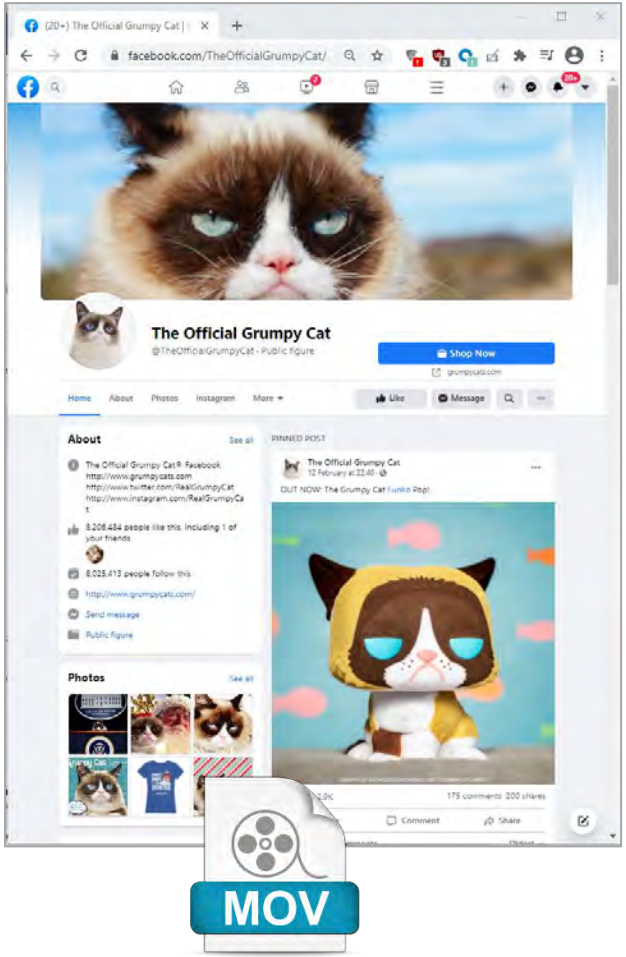
Screencast

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



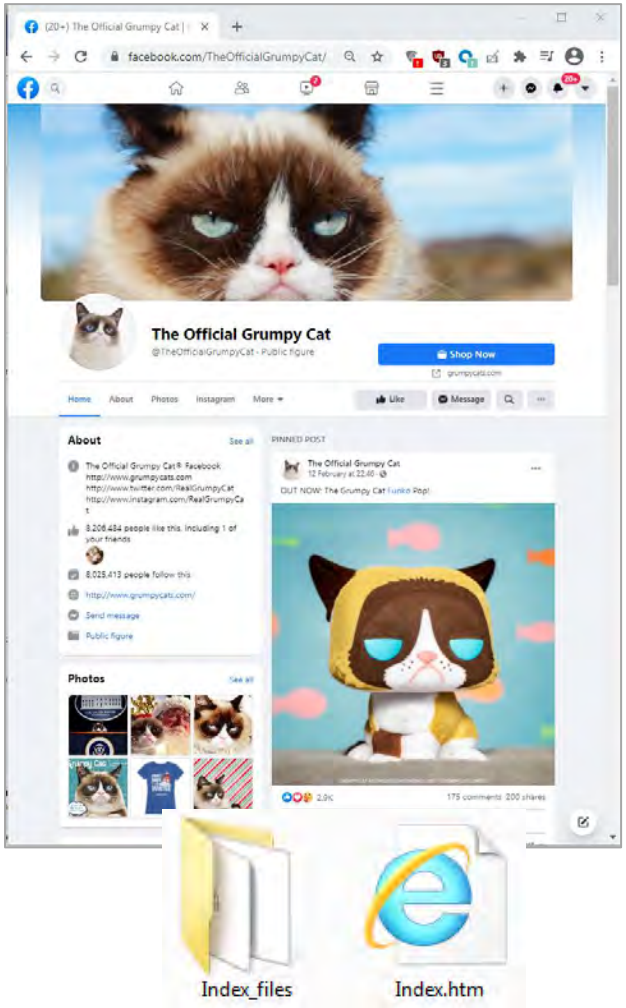
Save Webpage

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



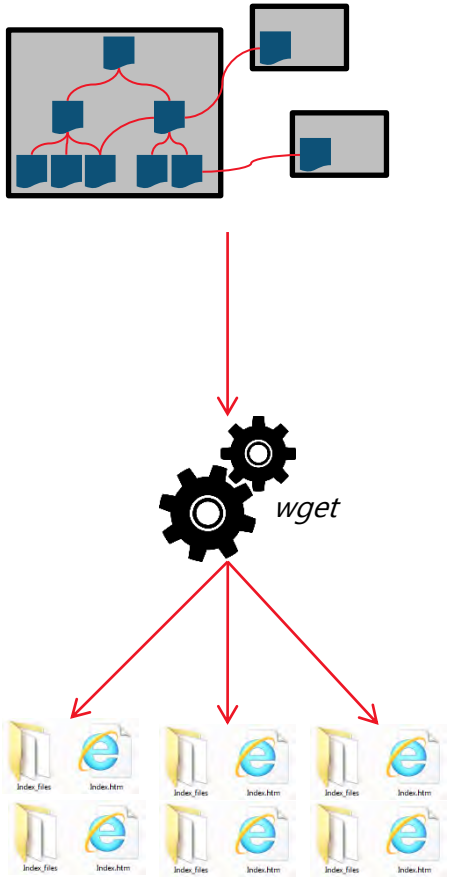
Save Script

Technique

- Download multiple pages all at once
- Can be tailored to follow any third-party links to download
- 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



Save Script

wget

-E	Adjust extension, save files properly
-p	Get all images needed to display the page
-k	Convert links to local pages
-r	Recursive download
-l 1	Go one Level deep
-U "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.79 Safari/537.36" --no-proxy	Pretend you are firefox. This makes the script declares itself as Firefox to stop web servers blocking unknown crawlers
--span-hosts	When recursing, go to external hosts if needed
--random-wait	Wait a random set of time before next request
"https://www.boards.ie/vbulletin/showthread.php?p=116450774"	The page we are downloading

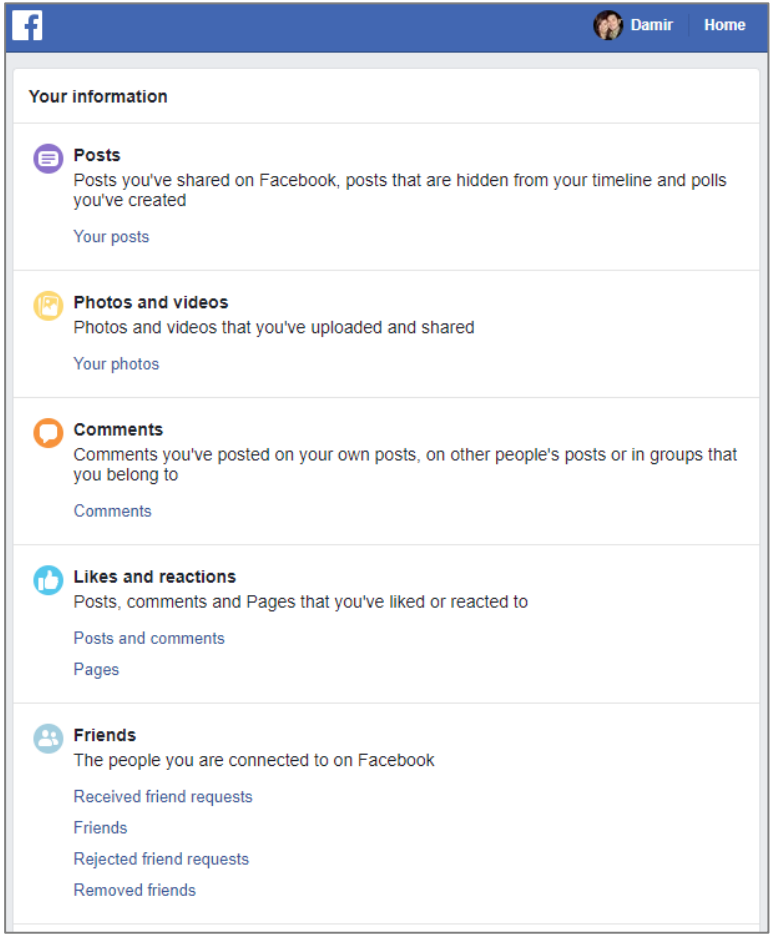
Data Export

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



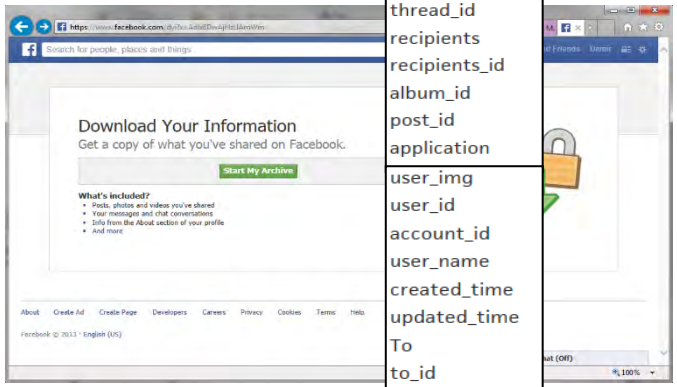
APIs

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

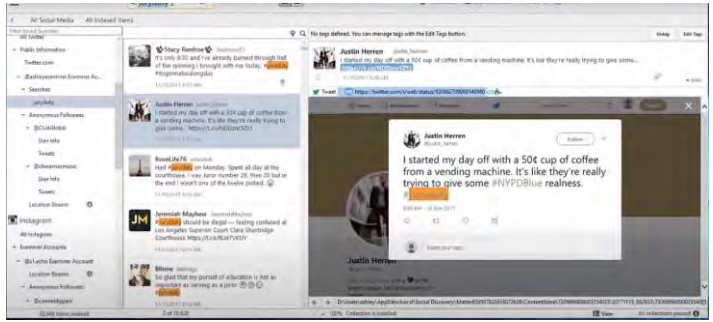


Metadata Field
Uri
fb_item_type
parent_itemnum
thread_id
recipients
recipients_id
album_id
post_id
application
user_img
user_id
account_id
user_name
created_time
updated_time
To
to_id
Link
comments_num
picture_url

APIs

X1 Discovery

- Supports: Twitter, Instagram, Facebook, Tumblr, YouTube and Online mail
- Downloads all components, hashes the files and maintains an audit trail
- Download all accessible information
- Requires a ‘dummy’ social user account to log into the social network
- Does not support forum downloads



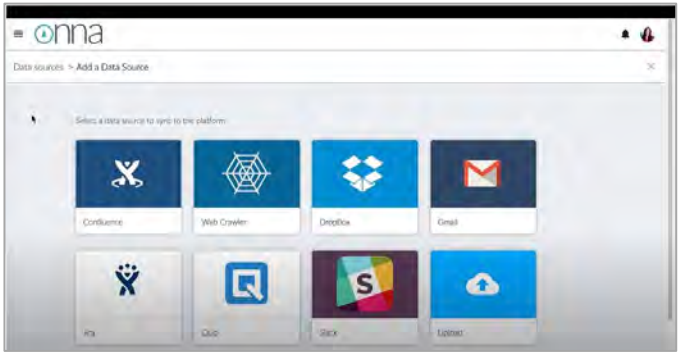
Magnet AXIOM

- Full fledged forensics software
- Support collections from Facebook only

APIs

Onna

- Support corporate social media preservation.
- Teams, Slack, Twitter, Confluence, Jira, Box, OneDrive, Sharepoint, etc.
- Downloads all components maintains an audit log
- Download all accessible information and presents it in a usable fashion



Hanzo

- Preservation software for eDiscovery and litigation
- Supports the same as Onna

- None support forum downloads other than as a webpage
- So what can we do about that?

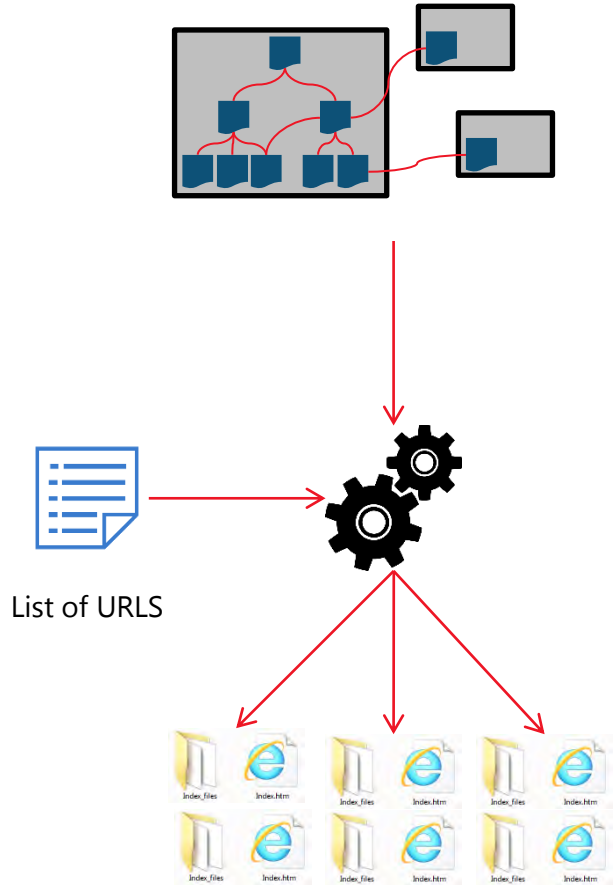
Forum Activity Download

Technique

- There is no automated way to gather all pages in one go
- List the URLs and use a webpage downloading tool to gather the lot

Problem

- You have to do this per website per thread manually!
- May be thousands of pages to visit
- Will make analysis difficult



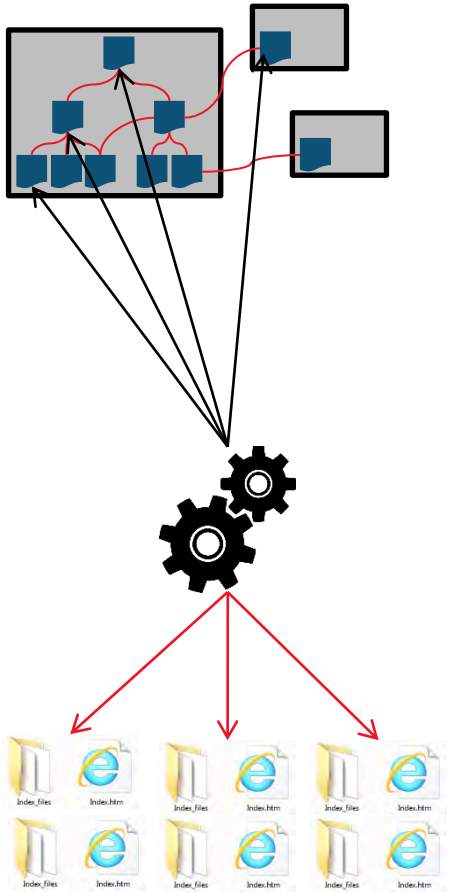
Screen Scraping

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

Problems

- Software needs to be created for every type of forum **vendor**
- May be blocked by the vendor



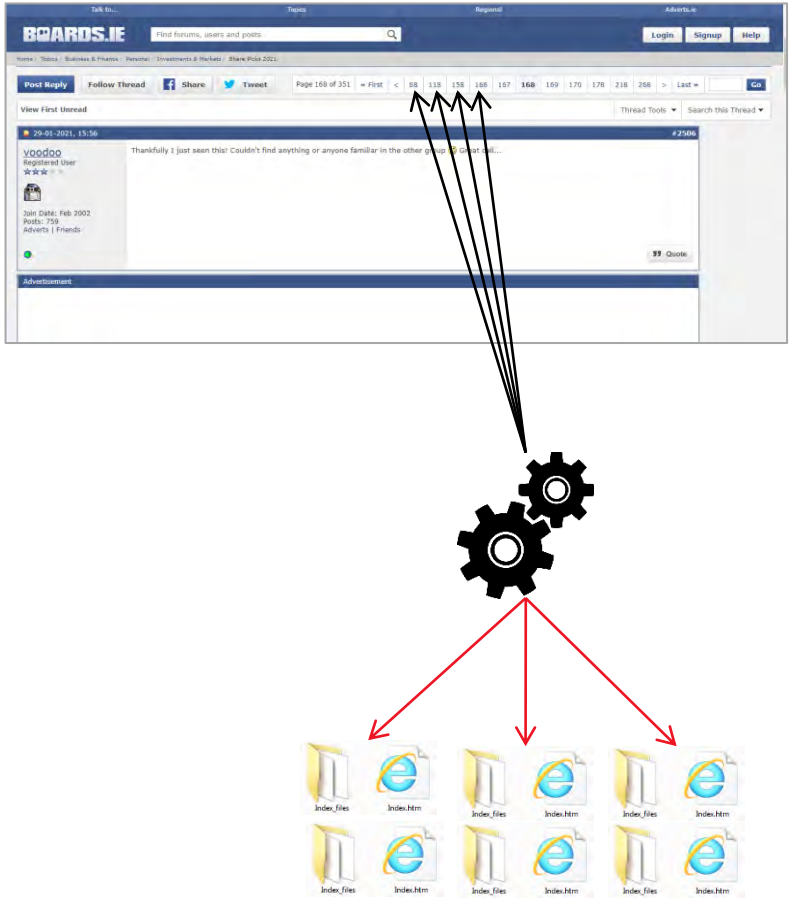
Screen Scraping

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

Problems

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



Summary

Technique	Prove Authenticity	Scalable?	Ease of Use?	Ease of Review?	Applicability
Screenshot	No	No	Yes	No	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

Review

Review Platforms

Social Media

Properly organised data makes it easy to review the documents in situ

Relationships between the posts \ users and threads can be maintained

Relativity is the leading review platform for document review

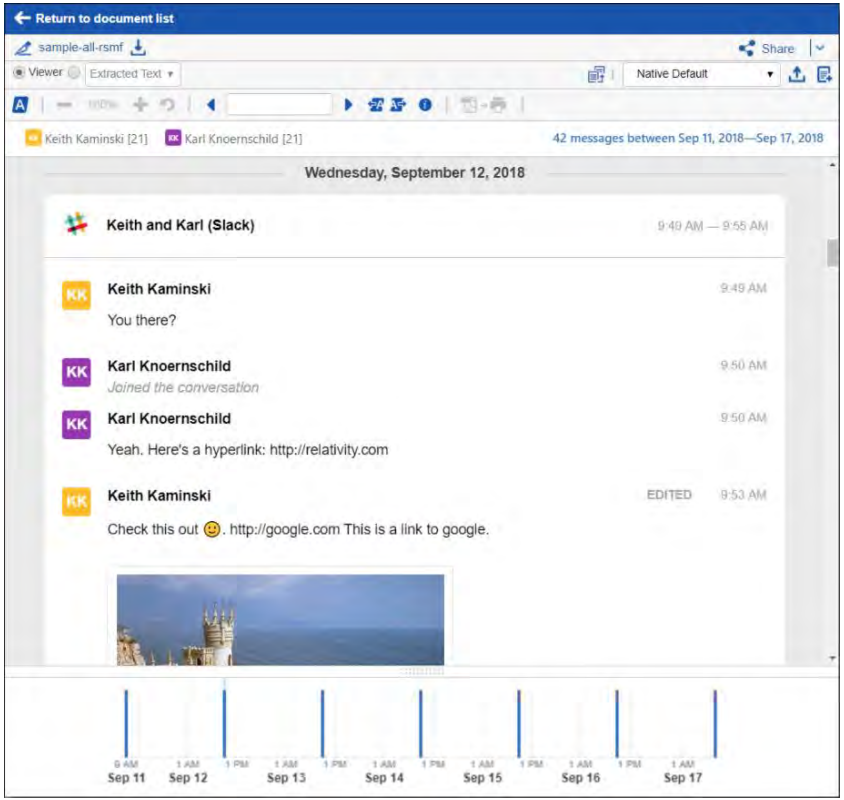
Review Platforms

RSMF

Add on for short message formats

Allows for Teams \ Slack and other messages to be reviewed in their native way

This is still a developing field of interest



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

Damir Kahvedžić | ProSearch | Solutions Advisor

Damir.Kahvedzic@prosearch.us

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

The European Investigation Order (EIO)

and its effectiveness in collecting e-evidence located abroad

Prof. dr. Joachim Meese
University of Antwerp
Attorney

Universiteit Antwerpen

The EIO Directive

Historical background

Universiteit Antwerpen

Historical background

- Abundance of traditional 'mutual legal assistance'-instruments:
  - Benelux Treaty of 1962
  - European Convention on Mutual Assistance in Criminal Matters of 1959
  - Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 1978
  - Convention implementing the Schengen Agreement of 1990
  - Naples II Convention of 1997
  - Convention on Mutual Assistance in Criminal Matters between the EU countries of 2000
  - Protocol to the Convention on Mutual Assistance in Criminal Matters between the EU countries of 2001
  - Second Additional Protocol to the European Convention on mutual assistance in criminal matters of 2001
  - Council Framework Decision on the execution in the European Union of orders freezing property or evidence of 2003
  - Benelux police cooperation treaty of 2004
  - Council Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union of 2006
  - Prüm Convention of 2008
  - Council Framework Decision on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters of 2008, ...

Historical background

- Challenge (particularly for e-evidence):
  - hard to get a timely response to a request
  - too much formalities
  - too complicated and technical to use
- 'Workarounds' to avoid MLA
  - e.g. Belgian jurisprudence regarding cooperation duties of service providers (cases of Yahoo and Skype)

Historical background

- The hoped-for solution: the EIO Directive of 3 April 2014, n° 2014/41/EU (EIOD)
  - proposed in April 2010 at the end of the Belgian Presidency
  - supported by a limited number of EU Member States:
    - » Austria, Bulgaria, Belgium, Estonia, Slovenia, Spain and Sweden
  - implementation by 22 May 2017 (but arduous)
    - » https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32014L0041
    - » https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat/EN/120
    - » Ireland and Denmark are not bound by the Directive;
    - » Recently also the United Kingdom which is already causing practical problems
      - » See UK Supreme Court 5 February 2021

The EIO Directive (EIOD)

Overview with a focus on e-evidence

Universiteit Antwerpen

Basic premise

- Replace existing legal framework by creating 1 single legal instrument (introductory remark 7 EIOD)
- Mutual recognition (art. 1(2) EIOD)

=> inspired by:

- mutual recognition of judgments and judicial decisions
- mutual recognition of orders to prevent the destruction, transformation, moving, transfer or disposal of evidence
- European evidence warrant
- European arrest warrant

The EIO Directive: *including e-evidence?*

- Applicable to any investigative measure (art. 3 EIOD):
  - including gathering of e-evidence
  - except in framework of Joint Investigation Team (JIT)
- In the context of e-evidence:
  - specific provisions on the interception of telecommunications (art. 30 EIOD)
  - no other specific provisions regarding electronic evidence
    - » except for a reference to the identification of a person holding an IP address or telephone number (art. 10(2)(e) EIOD)

The EIO Directive: *procedure*

1. National request prepared and judicially approved based on individual national standard and EIO rules (art. 5-6 EIOD)
   - particular form + content requirements: art. 5 EIOD + Annex A
   - translation of the EIO is required (art. 5, §3 EIOD)
2. EIO sent directly to relevant judicial authority in relevant country (art. 7 EIOD)
   - by any means capable of producing a written record to guarantee authenticity
   - via the telecommunications system of the European Judicial Network
   - via E-Codex (https://www.e-codex.eu)?

The EIO Directive: *procedure*

3. EIO examined by receiving judicial authority
   - verification of EIO (art. 5-6 EIOD)
   - verification of grounds of refusal
     - important in a cybercontext:
       - ✓ similar investigative measure exception (art. 11 (c) + (h) EIOD)
       - ✓ dual criminality exception (art. 11 (e) + (g) EIOD)
       - ✓ fundamental rights exception (art. 11 (f) EIOD)
4. Execution of EIO:
   - executed directly by domestic investigative authorities OR
   - EIO served and then executed (if possible) by third parties (e.g. service provider)
   - recourse to a different type of investigative measure (art. 10 EIOD)

The EIO Directive: *procedure*

4. Evidence is sent back to executing judicial authority (art. 13 EIOD)
5. Costs: art. 21 EIOD
   - borne by the executing State
   - if exceptionally high: possibility to share or modify

The EIO Directive: *timeline*

- In theory: within 120 days (art. 12 EIOD)
  - 30 days for Member States to decide to accept request
  - then 90 days to execute requested investigative measure
  - unless urgency
- But:
  - many consultation options (art. 6(3) EIOD, art. 7(7) EIOD), art. 10(4) EIOD, art. 11(4) EIOD, art. 21(2) EIOD)
  - grounds for non-recognition or non-execution (art. 11 EIOD)
  - grounds of suspension of transfer of evidence (art. 13(2) EIOD)
  - grounds for postponement of recognition or execution (art. 15 EIOD)
  - legal remedies (art. 14 EIOD)

The EIO Directive: *specific regimes*

- See Chapter IV EIOD
- Relevant from e-evidence perspective: *the interception of telecommunications* (chapter V)
  - art. 30 §§7-8 + 31 EIOD
  - important aspects from an e-evidence perspective:
    - EIO shall be sent to only one Member State if more Member States are available to provide technical assistance
    - possibility to request decoding or decrypting of the recording
      - BUT no obligation
    - notification of Member State where the subject of the interception is located from which no technical assistance is needed

The EIO Directive (EIOD)

Challenges in a digital era

Universiteit Antwerpen

Characteristics of e-evidence

- Volatile
- Cross-border
- Necessity for quick intervention
- Hard to locate and access evidence (e.g. in cases where the origin of cyber attacks or location of e-evidence is not (yet) known)

Important challenges for EIO:

See EU Commission Impact Assessment 2018

The EIO: challenges

- *Limited scope:*
  - No JIT
    - BUT useful to share information and data
    - BUT useful to collect e-evidence
  - Territorial limitations:
    - only EU countries
      - ⇒ no access to data held by service providers headquartered in non-EU countries
    - Ireland, Denmark and the UK are not bound by the Directive
      - ⇒ no access to data held by service providers headquartered in these countries
      - ⇒ particularly in Ireland & the UK a number of US service providers store data and have European headquarters
    - risk of forum shopping by LEA and perpetrators?

The EIO: challenges

- *Not adapted to complex e-evidence situations:*
  - situations where a number of information systems are used simultaneously in multiple jurisdictions to commit one single crime
  - situations where relevant e-evidence moves between jurisdictions in short fractions of time
  - situations where sophisticated methods are used to conceal the location of e-evidence or the criminal activity, leading to "loss of location"

The EIO: challenges

- *High cost and capacity requirements*
  - gathering e-evidence requires:
    1. significant investment of resources/capacity from the receiving Member State, which may not be appropriate or necessary for all cases, especially when there is no link with the receiving jurisdiction besides the seat of the service provider
       - ➢ risk of massive influx of requests to gather e-evidence
    2. specialised training/personnel required to collect e-evidence in an appropriate manner

The EIO: challenges

- *Too slow for e-evidence?*
  - as to interception of telecommunications: only send to 1 Member State
    <-> anonymous networks: hard to locate
  - in principle 120 days waiting period for the evidence
    - only option: EIOs in case of urgency but obligation to state reasons
  - many grounds for delay:
    - consultation options, grounds for non-recognition or non-execution, grounds of suspension of transfer of evidence, grounds for postponement of recognition or execution, legal remedies, ...

The EIO: challenges

- *Too formalistic for e-evidence?*
  - long EIO forms to be completed
    - standarised forms and procedures not adapted to securing and obtaining e-evidence
  - requirement to provide EIO translation
  - EIOs generally transferred by conventional postal delivery services
    - in urgent cases sometimes by e-mail
    - E-CODEX?
  - impossibility to directly address service providers

The EIO: challenges

- *Legal impediments*
  - on investigative acts-level:
    - risk for inconsistent interpretations
    - risk for conflicts between existing regulations
      - e.g.: dual criminality-requirements, domestic equivalent of investigative acts, ...
    - challenge to address the issue of non-disclosure of data requests
    - 'limitations' due to data protection (art. 20 EIOD) and fundamental rights requirements
      - e.g.: obligation to decrypt vs. privilege against self-incrimination

The EIO: challenges

- *Legal impediments*
  - on evidence level:
    - no 'free movement' of evidence or minimum standards for evidence-gathering
    - risk of important discussions on admissibility/authenticity of e-evidence in criminal procedures due to different domestic standards

The EIO: challenges

- *Remains too complex*
  - see art. 34 EIOD + introductory remark 8 EIOD
  - multiple legal instruments, agreements and arrangements remain applicable
    - see initial list of abundant instruments
- *Absence of overarching coordination mechanisms*

Way forward?

- European Production and Preservation Orders for electronic evidence?
  - see Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters of 17 April 2018
    - currently awaiting Parliament's position in 1st reading
    - https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0108(COD)&l=en
    - more attractive for law enforcement but less protective for persons concerned

Way forward?

- Combination of EIOD with more harmonisation + coordination?
  - Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings
    - https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2018:226:FIN

Way forward?

- Electronic user-friendly version of EIO forms
- A secure online platform for electronic exchanges of EIO requests

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

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

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**

The Timberline high bomb threats

“Have a nice exploding day”

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.

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)

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.

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. . . .

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.

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.

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...

football leaks

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 3

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)

TorBrowser | The Hidden Wiki | The Hidden Wiki | Welcome! | Silk Road | BlackMarket Reloaded v.3 -- Register

silkroadvb5piz3r.onion/index.php

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/
B20.19

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

Anti-forensic techniques

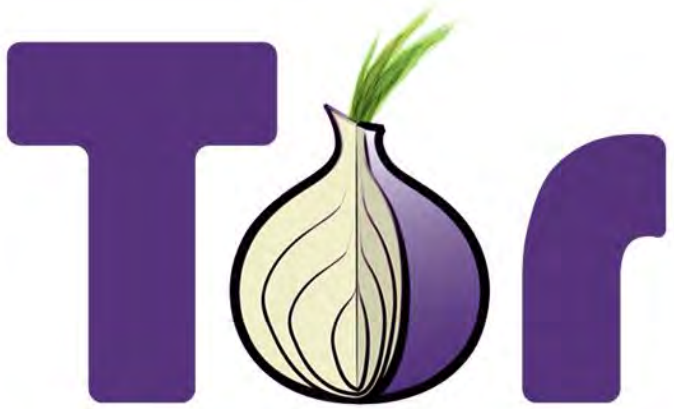
Multiple internet access locations

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.

Anonymizing tools



Following the (virtual) money

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

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

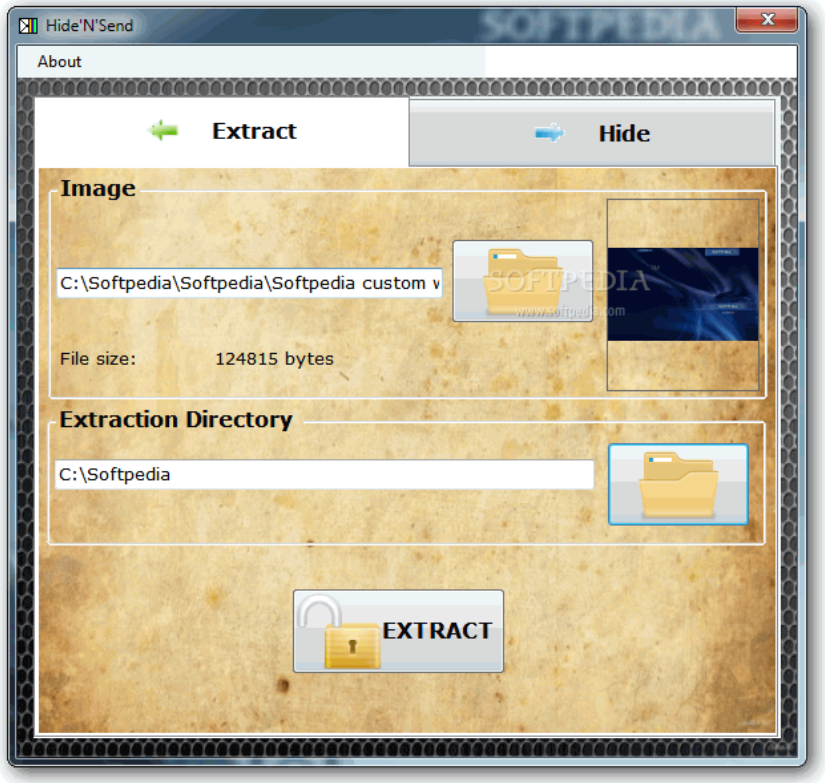
WASHINGTON – Nicodemo S. Scarfo, the son of Philadelphia's former mob boss, was almost paranoid enough.

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.

Steganography



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.

Other difficulties in finding and collecting digital evidence

Jurisdictional challenges

Feds Out-Hack Russian Hackers

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

Comment / Share / Tweet / Stumble / Email

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)

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

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."*

Online undercover investigations

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?

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.

Different personas of the undercover agent

Using other **people's** credentials

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.

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.

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.

The use of malware and legal hacking to collect evidence

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.

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.

Minimum legal requirements

- 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

- 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.

Legal safeguards, reliability and the right of defence

Reporting

«***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.

Disclosure

- 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.

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.

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.

Thank you!

David Silva Ramalho
dsramalho@mlgts.pt

ERA 2021

OPEN SOURCE TOOLS, COMPUTER FORENSICS IN THE "CLOUD"

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

Encryption

Question

Are encryption and password protection the same thing?

a) YES

b) NO

Encryption

- Converting information from its normal, understandable form into an incomprehensible format that can normally only be interpreted (or decrypted) by using some form of secret knowledge

- Conversion of data into a form, called cipher text, which cannot be easily understood by unauthorized people

Terminology

Plaintext

Original message

Algorithm

- Method how to change plaintext

Key

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

Cipher Text

- Scrambled message

How does it work?

- Encryption allows the sender to transform data from **plain text** into **ciphertext** by using a **key**
  - **Ciphertext:** coded text
  - **Key:** what is used to encrypt and decrypt text

What is Encryption?

- Encryption: coding text
- Decryption: decoding text

- A security method used to protect data
  - Files on computers
  - Data being passed through the Internet
  - ATM machines
  - E-Commerce
  - Storage devices

Why Do We Use Encryption?

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

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

Types of encrypted evidence

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

Two sides to encryption

- The bad
  - Data is inaccessible to law enforcement
  - Criminal usage
  - Hard to recover if keys are lost or unobtainable
  - Everything is becoming more and more encrypted
  - Ransomware

- The good
  - Makes our data secure
  - Makes our connections secure
  - Low chance of data theft
  - Privacy and security aspects
  - Data validation

Use of entropy to discover encryption

- **Entropy** - concept or ameasurable physical property that is most associated with a state of disorder, randomness
- More entropy a password has, the stronger it tends to be
- Entropy increases with the length of the password and the variation of the characters that comprise it
- *Length* more significant
  - As the password gets longer, the number of new combinations gets exponentially larger
    - Much harder to guess

Encryption – forensic challenges

- Legislations
  - Don’t really help
  - Today is more about privacy and data security
  - **In general** there are no laws that would make someone provide their password/encryption key
    - In some countries it is also against the law to do so – testifying against yourself
  - There are some exceptions if crimes are related to terrorism or child exploitation
  - Some countries will fine you if you are accused and you don’t provide password/encryption key
  - Becomes extra complicated if there is also cloud service involved or non resident data storage

Dealing with encryption

- What can law enforcement do against encryption
  - Tools for detection
  - Doing a RAM dump on a live system to get the key
  - Live acquisition if file/drive is open/mounted before evidence seizure or pulling the plug
  - Get information about the suspect and use it for dictionary attack against encrypted data
    - Finding old password's and running it against encrypted data
  - Speak to vendor or system administrator
  - Look for tool/implementation weaknesses
  - Use supercomputers for password recovery and hope for the best ☹

Reverse image search

Question

It is possible to do a web search using images, not only words.

a) True

b) False

Reverse image search

- This is a search engine technology called Content Based Image Retrieval (CBIR) that can query image files as a normal search entry and returns information related to the image

- Reverse image search can be used to:
  - Locate the source of an image
  - Find higher resolution videos
  - Discover webpages on which the picture appears
  - Find the content creator
  - Get information about an image

Reverse image search

- Image search engines:
  - Google
  - TinEye
- Websites that provide reverse image search
  - Reddit
  - Karma Decay

Exercise (Image search engines)

- Use Google and TinyEye
  - Compare the search results:
    - 1975 Datsun 280z

Google search results

Google 1975_...n_280z.jpg 1975 datsun 280z

All Images Maps More Settings Tools

About 255 results (1.12 seconds)

Image size:
940 × 627

Find other sizes of this image:
All sizes - Medium

Possible related search: ***1975 datsun 280z***

www.hagerty.com › apps › valuationtools

1975 Datsun 280Z Values | Hagerty Valuation Tool®

The real solution to emission laws came with the introduction of the fuel injected **280Z** in **1975**. The addition of a license-built Bosch L-Jetronic injection to the ...

www.automobile-catalog.com › make › datsun

1975 Datsun 280Z Coupe (S30) full range specs

All **Datsun 280Z** Coupe (S30-series) versions offered for the year **1975** with complete specs, performance and technical data in the catalogue of cars.

Visually similar images

Report images

Pages that include matching images

bringatrailer.com › ... › Auctions › 1975 Datsun 280Z

1975 Datsun 280Z for sale on BaT Auctions - sold for $15,500 ...

940 × 627 — Bid for the chance to own a **1975 Datsun 280Z** at auction with Bring a Trailer, the home of the best vintage and classic cars online. Lot #33391.

TinyEye search results

TinEye

Search Technology Products About Log in

Upload Paste or enter image URL

1 result

Searched over 46.1 billion images in 2.3 seconds for:
lh3.googleusercontent.com/8BxnToGIVZIMq0zsx8DRlzQrBUIX3...

Using TinEye is private. We do not save your search images. TinEye is free to use for non-commercial purposes. For business solutions, learn about our technology.

Sort by best match

Filter by domain/collection

hiveminer.com

Tags/arizona,cars - First found on Feb 7, 2020

Filename: **49451678641_90610547f2_b.jpg** (1024 x 683, 253.2 KB)

INSIG2

Revers image searching with Browser add-on’s

Search by Image

Available in the Chrome Web Store

GET THE ADD-ON

Get it from Microsoft

Get it from Opera add-ons

Available on Galaxy Store

Download on the Mac App Store

Exchangeable image file format

- EXIF is a standard that specifies the format for interchange information of images that use JPEG compression by digital cameras, smartphones…

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

Exercise (EXIF data analysis)

- Use Pic2map website to find information:
  - 20200620_213359.jpg

Pic2map results

Pic2map results

CAMERA INFORMATION

Brand: Samsung	Model: SM-G985F	Lens Info: Unknown
Shutter: 1/4 (0.25 seconds)	F Number: f/2.2	ISO Speed: ISO 320
Flash: Not Used	Focal Length: 2.2 mm	Color Space: sRGB

FILE INFORMATION

File Name: 20200620_213359.jpg	Image Size: 4032 x 1816 pixels	Resolution: 7.3 megapixels
Unique ID: R12XLMF01CM	MIME Type: image/jpeg	Dots/Inch: 72 DPI

DATE & TIME

Date: 2020-06-20	Time: 21:34:06 (GMT +01:00)	Time Zone: Europe / Sarajevo

GPS INFORMATION

Latitude: 43.755834	Longitude: 15.784772	Lat Ref: North
Long Ref: East	Coordinates: 43° 45' 21.00" N , 15° 47' 5.18" E	Altitude: 0m. (Above Sea Level)
Direction Ref:	Direction:	Pointing:

LOCATION INFORMATION

City: Vodice	State: Vodice	Country: Croatia

Address: Miramare, Ulica Ljudevita Gaja, Vruje, Vodice, Grad Vodice, Šibenik-Knin County, 22211, Croatia

(Location was guessed from coordinates and may not be accurate.)

ExifInfo.org

Exif Info: 20200620_213359.jpg

Show location on map »

File

Filename
20200620_213359.jpg

File Size
2.2 MB

File Type
JPEG

File Type Extension
jpg

MIME Type
image/jpeg

Exif Byte Order
Little-endian (Intel, II)

Image Width
4032

Image Height
1816

Encoding Process
Baseline DCT, Huffman coding

Bits Per Sample
8

Color Components
3

Y Cb Cr Sub Sampling
YCbCr4:2:0 (2 2)

EXIF

Image Width
4032

Image Height
1816

Make
samsung

Camera Model Name
SM-G985F

Orientation
Horizontal (normal)

X Resolution
72

Y Resolution
72

Resolution Unit
inches

Software
G985FXXU2ATE6

Modify Date
2020:06:20 21:34:06

Y Cb Cr Positioning
Centered

Exposure Time
1/4

F Number
2.2

Exposure Program
Program AE

ISO
320

Exif Version
0220

Date/Time Original
2020:06:20 21:34:06

Create Date
2020:06:20 21:34:06

Shutter Speed Value
0.8

Aperture Value
2.2

Exposure Compensation
0

Max Aperture Value
2.2

Metering Mode
Center-weighted average

Flash
No Flash

Focal Length
2.2 mm

Color Space
sRGB

Exif Image Width
4032

Exif Image Height
1816

Exposure Mode
Auto

White Balance
Auto

Digital Zoom Ratio
1

Focal Length In 35mm Format
13 mm

Scene Capture Type
Standard

Image Unique ID
R12XLMF01CM

GPS Latitude Ref
North

GPS Latitude
43 deg 45' 21.00"

GPS Longitude Ref
East

GPS Longitude
15 deg 47' 5.18"

Compression
JPEG (old-style)

Thumbnail Offset
868

Thumbnail Length
31989

Thumbnail Image
[binary data]

MakerNotes

Time Stamp
2020:06:20 15:34:06-04:00

Composite

Aperture
2.2

GPS Latitude
43 deg 45' 21.00" N

GPS Longitude
15 deg 47' 5.18" E

GPS Position
43 deg 45' 21.00" N, 15 deg 47' 5.18" E

Image Size
4032x1816

Megapixels
7.3

Scale Factor To 35 mm Equivalent
5.9

Shutter Speed
1/4

Circle Of Confusion
0.005 mm

Field Of View
108.3 deg

Focal Length
2.2 mm (35 mm equivalent: 13.0 mm)

Hyperfocal Distance
0.43 m

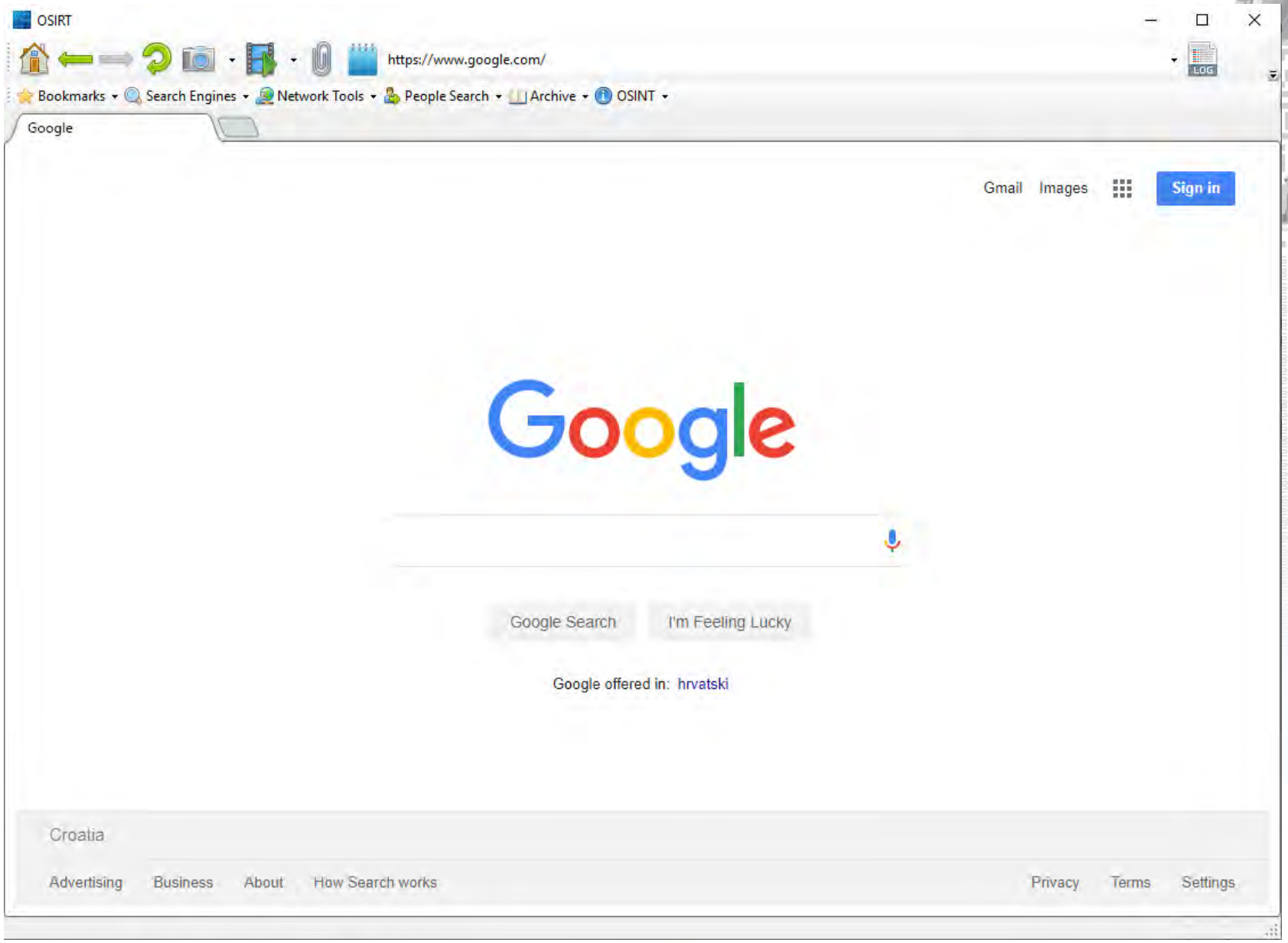
Light Value
2.6

How to review an offline webpage

Examining web-pages

- Great tool to examine webpages is Open Source Internet Research Tool (OSIRT)
- Works only on Windows
- Features of OSIRT:
  - Built in video and screenshots capture tools
  - Webpage download
  - Uses Tor o protect your identity
  - Creates reports
  - Automated logging
  - Case notes

OSIRT exercise



Reviewing old/offline web-pages

- To analyze an offline or old version of a web-page WayBackMachine can be used
- WayBackMachine is an archive of website snapshots
- Is also integrated in to OSIRT browser

DONATE

INTERNET ARCHIVE WayBackMachine

Explore more than 371 billion web pages saved over time

Enter a URL or words related to a site's home page

Feedback

Tools

Wayback Machine Availability API

Chrome Extension

Firefox Add-on

Safari Extension

iOS app

Android app

Subscription Service

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. Visit Archive-It to build and browse the collections.

Save Page Now

https://

SAVE PAGE

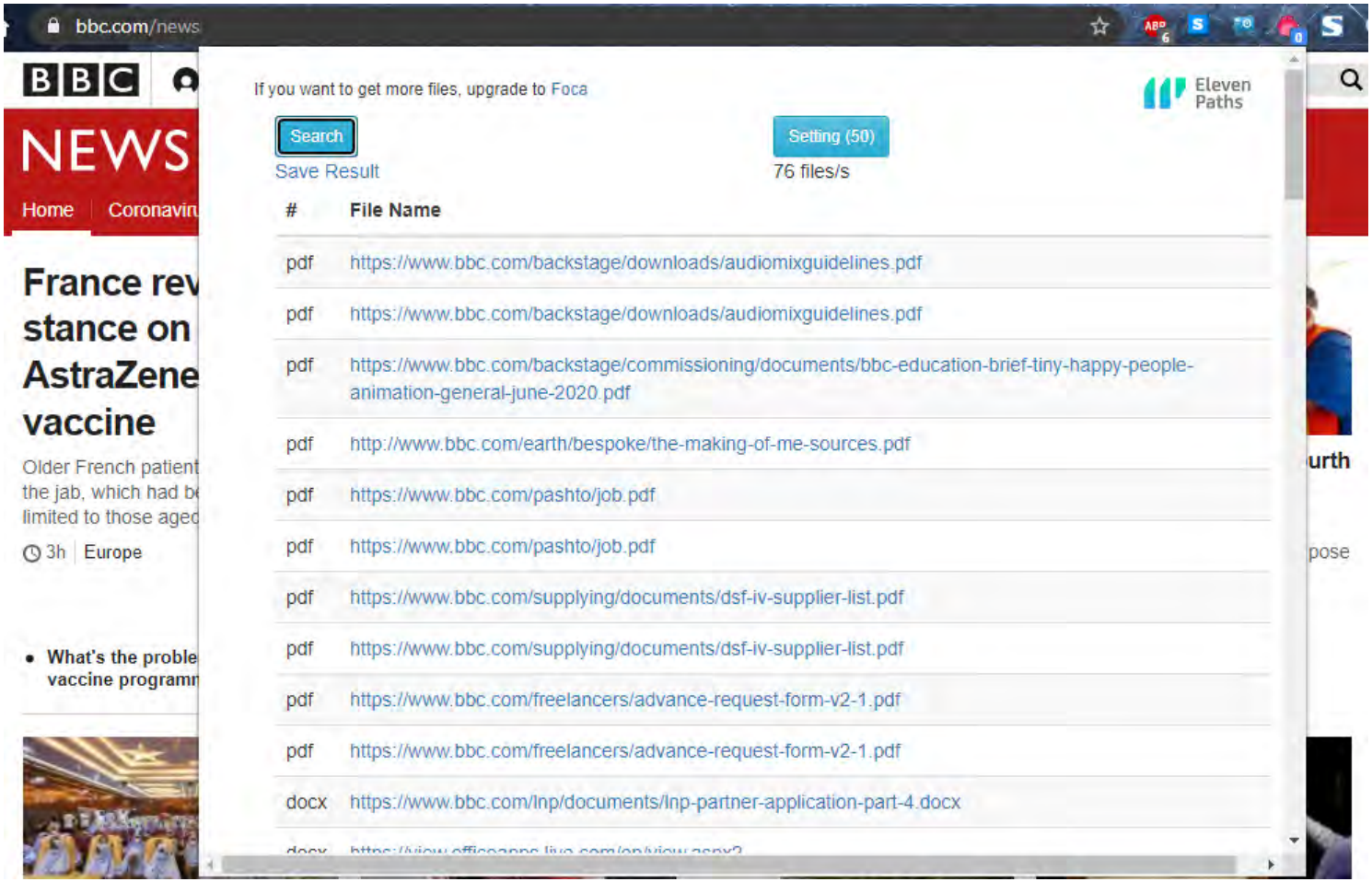
Capture a web page as it appears now for use as a trusted citation in the future.

Try New Version! (beta)

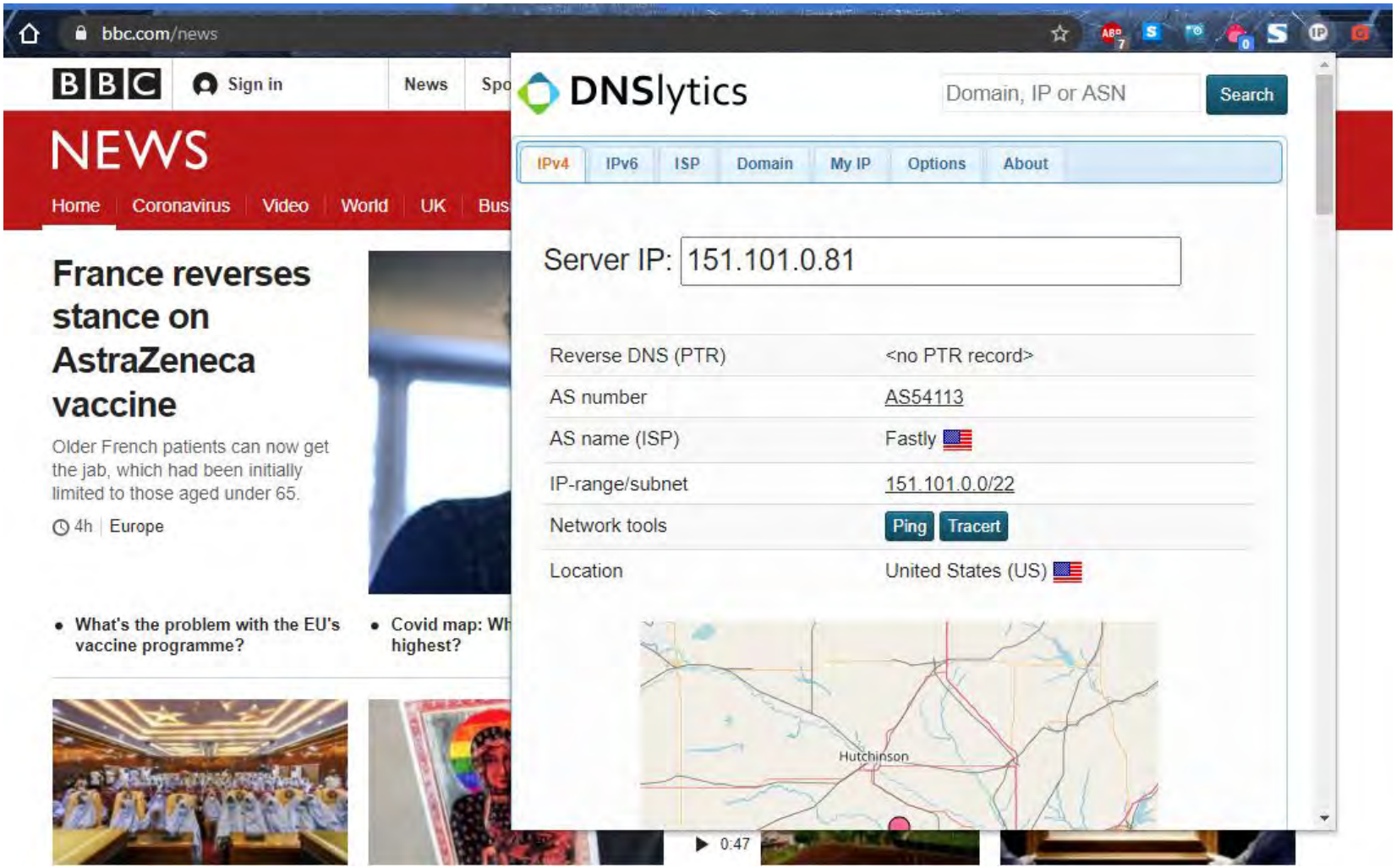
Analyzing webpages using add-on's

- Foca Files Finder
  - Foca Files Finder uses Bing to search for documents hosted in a domain
  - The plugin will show all documents hosted in a domain, thanks to Bing technology
  - Export, if you want to, results to a file and use them in FOCA
- IP address and domain information
  - shows detailed information about every IP Address, Domain Name and Provider
- Fire Shot
  - performs full page screen capture
  - creats PDF files from web pages

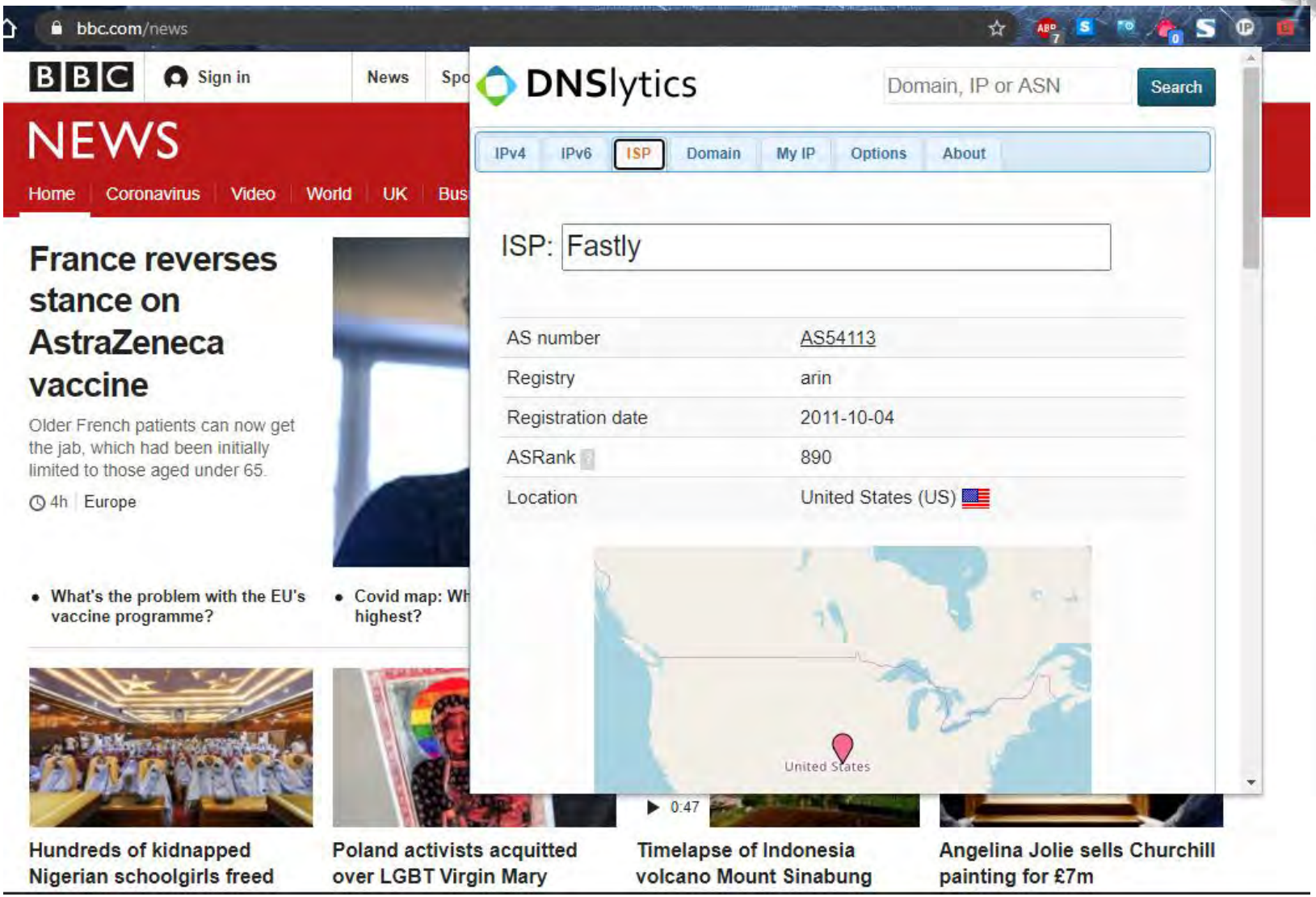
Foca Files Finder



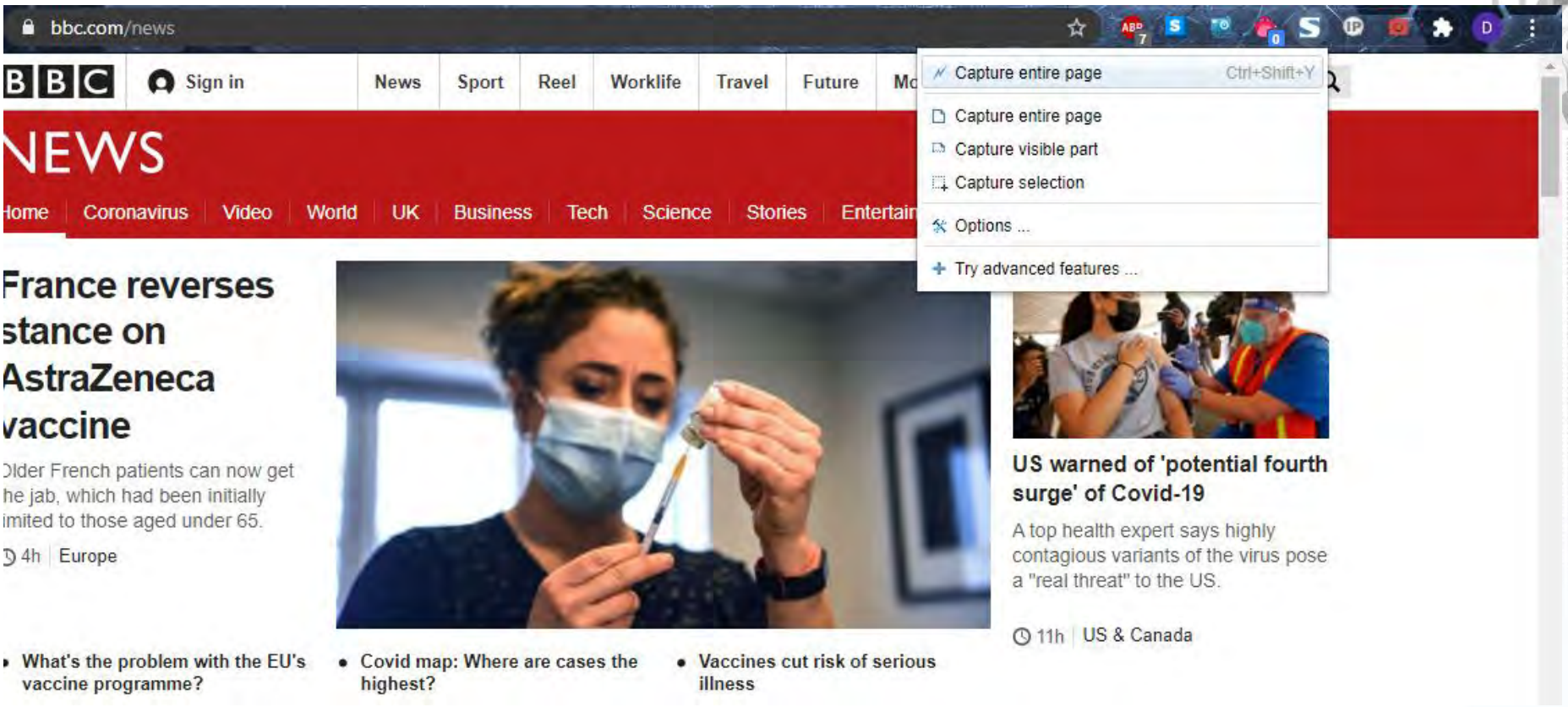
IP address and domain information



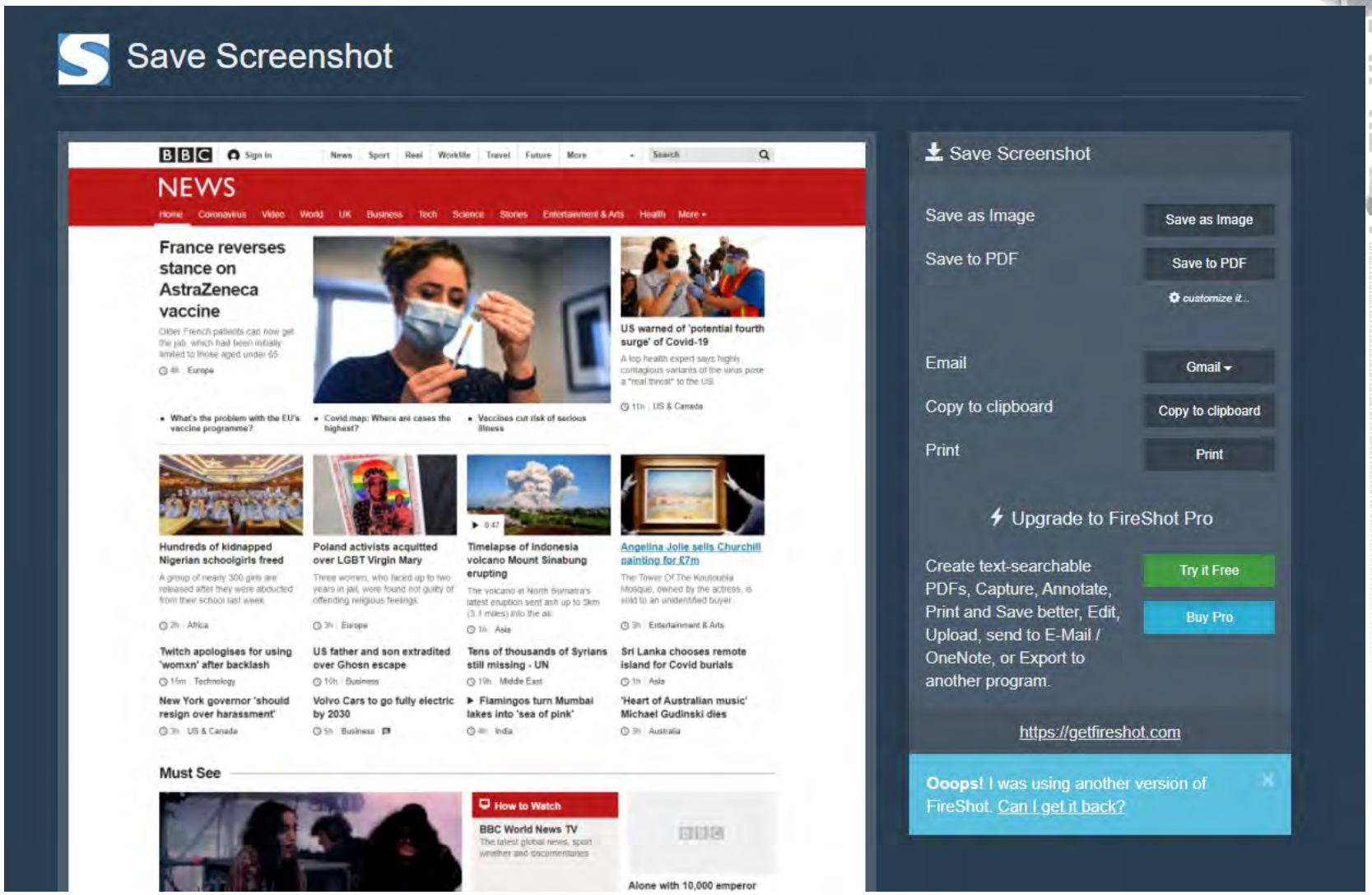
IP address and domain information



Fire Shot


bbc.com/news
BBC
Sign in
News
Sport
Reel
Worklife
Travel
Future
Capture entire page Ctrl+Shift+Y
Capture entire page
Capture visible part
Capture selection
Options ...
Try advanced features ...
NEWS
Home
Coronavirus
Video
World
UK
Business
Tech
Science
Stories
France reverses stance on AstraZeneca vaccine
Older French patients can now get the jab, which had been initially limited to those aged under 65.
4h | Europe
US warned of 'potential fourth surge' of Covid-19
A top health expert says highly contagious variants of the virus pose a "real threat" to the US.
11h | US & Canada
What's the problem with the EU's vaccine programme?
Covid map: Where are cases the highest?
Vaccines cut risk of serious illness

Fire Shot


Save Screenshot
BBC
Sign in
News
Sport
Reel
Worklife
Travel
Future
More
Search
NEWS
Home
Coronavirus
Video
World
UK
Business
Tech
Science
Stories
Entertainment & Arts
Health
More
France reverses stance on AstraZeneca vaccine
Older French patients can now get the jab, which had been initially limited to those aged under 65
4h Europe
US warned of 'potential fourth surge' of Covid-19
A top health expert says highly contagious variants of the virus pose a "real threat" to the US
11h US & Canada
What's the problem with the EU's vaccine programme?
Covid map: Where are cases the highest?
Vaccines cut risk of serious illness
Hundreds of kidnapped Nigerian schoolgirls freed
A group of nearly 300 girls are released after they were abducted from their school last week
2h Africa
Poland activists acquitted over LGBT Virgin Mary
Three women, who faced up to two years in jail, were found not guilty of offending religious feelings
3h Europe
Timelapse of Indonesia volcano Mount Sinabung erupting
The volcano in North Sumatra's latest eruption sent ash up to 3km (1.1 miles) into the air
1h Asia
Angelina Jolie sells Churchill painting for £7m
The Tower Of The Koutoubia Mosque, owned by the actress, is sold to an unidentified buyer
3h Entertainment & Arts
Twitch apologises for using 'womxn' after backlash
15m Technology
US father and son extradited over Ghosn escape
10h Business
Tens of thousands of Syrians still missing - UN
19h Middle East
Sri Lanka chooses remote island for Covid burials
1h Asia
New York governor 'should resign over harassment'
3h US & Canada
Volvo Cars to go fully electric by 2030
5h Business
Flamingos turn Mumbai lakes into 'sea of pink'
4h India
'Heart of Australian music' Michael Gudinski dies
3h Australia
Must See
How to Watch
BBC World News TV
The latest global news, sport, weather and documentaries
Alone with 10,000 emperor
Save Screenshot
Save as Image
Save as Image
Save to PDF
Save to PDF
customize it...
Email
Gmail
Copy to clipboard
Copy to clipboard
Print
Print
Upgrade to FireShot Pro
Create text-searchable PDFs, Capture, Annotate, Print and Save better, Edit, Upload, send to E-Mail / OneNote, or Export to another program.
Try it Free
Buy Pro
https://getfireshot.com
Ooops! I was using another version of FireShot. Can I get it back?

Physical and logical acquisition of data

Data acquisition

- Retrieving evidence data from various types of media
- Acquisition tools – software (forensic imaging programs)/hardware (write blockers, forensic duplicators, other forensic devices)
- Forensic boot environment
- Validation is necessary
- Destination media – hard disk drives for storing forensic backups
  - Media sterilization

Data acquisition

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

Sterile media

- As we know, even after deleting files there is data left over
- If destination disks for forensic backups contain leftover data from earlier, it could be mistaken for evidence
- → Sterile media
- Sterile media has every byte overwritten with a known or random hex value
- Forensically sterile media → Every byte has the value of 0x00
- Sterilization = wiping

Physical image

- Physical image:
  - Will capture all ones and zeroes on a drive
  - It will create an identical copy of the source drive
  - Copy's free space on the drive
  - **Captures deleted files and fragments of a drive**(even of it was recently formatted)
  - 1TB of source drive requires the same or more free space on the destination drive

Logical image

- Logical image:
  - Will capture all active data (the same as using File Explorer)
  - Does not capture deleted files or free space
  - If imaging a 1TB drive that only has 30GB of active data/files, the destination drive will only need 30GB
  - **Used to image encrypted drives!!**

Cloud providers and replicated data on websites

Cloud forensics

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

Question

Data can be seized from cloud the same way as in regular computer forensics.

a) True

b) False

Traditional vs cloud forensics

- Identification of potential evidence
  - Storage networking and virtualization makes mapping storage devices complex
- Acquisition
  - Not possible to access physical incident scene
  - Not physical but logical items
    - Virtual hard disk file, file that contains server memory…
    - “powered off” devices physically invisible
- Not auditable
  - Investigations on dynamic systems that can’t be frozen
  - Documentation and expertise
- Virtualization layer might add time drift

Cloud forensics

Multi-dimensional issue

- Remote forensics
- Live forensics
- Virtual acquisition
- Network forensics

Social networks

Web browser & OSINT

E-mails

File - sharing network & **Cloud**

Forum & Blog

Chat

Physical inaccessibility

- Evidence can be spread all over the world
- Decentralized logs
- Virtual instances may migrate transparently between physical instances with little recordkeeping
- Problems:
  - ACQUISITION: Gathering data
    - Evidence needs to be provided by Cloud Service Provider
    - Located in multiple data centres around globe
  - AUTHENTICATION: User's data kept together with other user's data on same storage system, hard to separate

Large amount of data

- Storage space
  - Big
  - Cheap
  - Easy to deploy
- Acquisition and processing time increased
- Lot of information to analyse
- VM instance size increases with amount of data in VM
  - To get data, VM instance image needs to be downloaded
    - Requires adequate bandwidth
    - Challenge with time critical cases

Why is evidence from social networks hard to collect?

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

Why is evidence from social networks hard to collect?

- Information credibility
  - Can be manipulated
    - E.g. Facebook check-in
  - Expert can get information but not be sure information is true
  - Possible to obtain information directly from social network
- Information sensitivity
  - Can be deleted at any time by user
- Information copying
  - Can be easily copied to storage device or saved as screenshot

Chain of custody

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

Cross border law

- Multi-jurisdictional and multi-tenancy
- Data centres located across the world
- Its up to cloud providers to comply with local laws;
  - But its up to local jurisdictions to ensure accurate and righteous laws
- Cloud computing – grey area of Law

Trustworthy data retention

- One of the mandatory compliance issues that has direct impact on digital forensics
- Should provide the long-term retention and disposal of organizational record
- Who enforces the retention policy in the cloud?
- How can the CSPs assure us that they do not retain data after destruction of it?

Presentation in the court of law

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

Cloud forensics challenges

- Jurisdiction
- Lack of international collaboration
- Investigating external chain of dependencies of the cloud provider
- Lack of law/regulations
- Decreased access to and control over forensic data at all levels of customer side

Solutions

- International cooperation
  - Global unity
- Trans-border access to stored computer data
- 24/7 network
- Interdepartmental support
- Team work
- Constant education
  - How to seize, acquire, process and store digital evidence
  - Laws

Thank you!

danijel.sladovic@insig2.com

INSIG2

Faculté de Droit,
d'Économie
et de Finance

The collection of evidence located abroad and the challenges of cross border access to data

Assoc. Prof. Dr. Stanislaw Tosza

08 March 2021

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

Criminal investigation in cyberspace

- **Cross-border access to data**
  - The need to gather/have access to data
- **Cloud computing**
  - The problem of territoriality
- **European enforcement challenges in the online context**
  - Conflicting rules
  - Yahoo and Skype cases
- **Shortcomings and remedies**
  - Shortcoming of the MLA system
  - EIO – a remedy for e-evidence?
  - EPOR – proposal, negotiations and future

Criminal investigation in cyberspace

- Need to gather data
- Role of data in global economy and private life
- Ability to combat crime – ability to to access data
- Not only cybercrime

Territoriality and limits of enforcement

- Territoriality – concept
- Jurisdiction to prescribe
- Jurisdiction to enforce
- France v. Turkey (S.S. Lotus):

  [45] “The first and foremost restriction imposed by international law upon a State is that – failing existence of a **permissive rule to the contrary** – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention”.
- Ex. of exception: Art. 41 CISA

Criminal investigation in cyberspace – Jurisdiction – Cybercrime convention

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

A Party may, without the authorisation of another Party:

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

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

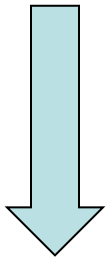
European enforcement challenges

Territoriality

Loss of location

Encryption problem

Enforcement capacity limitation



Cooperation of service providers

European enforcement - legal challenges

- **Mutual legal assistance and its shortcomings**
  - Functioning of the MLA system
  - MLA for data and US: probable cause
- **Problem of cooperation with the US: the blocking provision**
  - 18 U.S.C. § 2702
  - Content data vs Non-content
  - Microsoft Ireland Case
- **Unilateral / extended jurisdiction – "Belgian approach"**
  - Yahoo case
  - Skype case
  - Code d'instruction criminelle

European enforcement – solutions?

- **Voluntary cooperation**
  - Practice
  - Problems
- **European Investigation Order**
- **E-evidence initiative**
  - European Production/Preservation Order Regulation (EPOR)
  - Directive on appointment of legal representatives
- **Solution to the US problem of the blocking provision**
  - CLOUD Act
  - US-UK Agreement
- **Second Protocol to the CoE Cybercrime Convention**

Getting data under European Investigation Order

- European Investigation Order – a general instrument to gather data cross-border within the EU
- Mutual recognition
- EIO is a judicial decision to have specific investigative measure(s) carried out in another MS with the objective to obtain evidence
- Production orders?
- Issuing authority and addressee (executing authority)
- Measure must be available in the issuing state and ordered under the same conditions as would be necessary to its issuance in a similar domestic case.
- Necessity and proportionality
- Deadlines: 30 days and 90 days
- Grounds for refusal
- Remedies

European Production/Preservation Order

The justification for the need for a EU setting

- Internal EU reasons
- External reasons ⟹ Negotiations with the US

Basic premises of the new system

- Mutual recognition
- Area of Freedom, Security and Justice (taken seriously)
- Lack of territoriality as principle

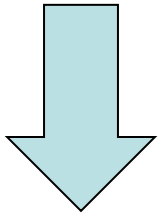
European Production/Preservation Order

State of play:

EU Commission's proposal – 04.2018

EU Council's General Approach – 12.2018

Position of the EU Parliament – 12.2020



Trialogue negotiations

European Production Order – Issuing

1. **Categories of data**
    - subscriber data
    - access data
    - transactional data
    - content data
2. **Issuing authorities**
    - judge
    - court
    - investigating judge
    - prosecutor
3. **Conditions of issuing**
    - necessary and proportionate
    - availability of a similar measure in the national system
    - type of offence (transactional data or content data)

European Production Order – Reaction

4. Reception

- legal representatives
- Directive
- consequences of lack of legal representative

5. Reaction

- Production of data
- 10 days/6 hours
- Problems with identifying / producing data

European Production Order – enforcement

6. Enforcement

- Enforcing State/authority
- Grounds for refusal

7. Sanctions

- Pecuniary
- Member States
- Who?

European Production Order – remedies

8. Remedies

- Member States
- Undefined

9. Conflict with other legal systems

- Problem
- Procedure

European Production Order – assessment

Positives:

- Solution
- Legal framework
- Time

Problems (some…):

- Mutual trust / legal basis
- Position of the service provider
  - Conflict of laws
  - Human rights choices
- Sanctions
- Remedies
- Relationship with the European Investigation Order

European Production Order – assessment

EU Parliament's position – trying to address some problems – some key differences:

- No Directive – included into Regulation
- obligatory notification of the state where the order is addressed
  - subscriber data and IP addresses – no suspensive effect
  - traffic and content data – suspensive effect
  - issuing State subject to Article 7 TUE procedure - explicit written approval

Main question

- Do we need this instrument?
- Relationship with the European Investigation Order
  - "*All evidence is equal, but electronic evidence is more equal than any other*" NJECL 2/2020, https://journals.sagepub.com/doi/full/10.1177/2032284420919802
- Importance of the agreement with the US

CoU – Cybercrime Convention

- 2nd Additional Protocol to the Budapest Convention on Cybercrime

- Direct disclosure of subscriber information

- Ongoing negotiations

Faculté de Droit,
d'Économie
et de Finance

Assoc. Prof. Dr. Stanislaw Tosza

The collection of evidence located abroad and the challenges of cross border access to data

Thank you for your attention !!

Questions?