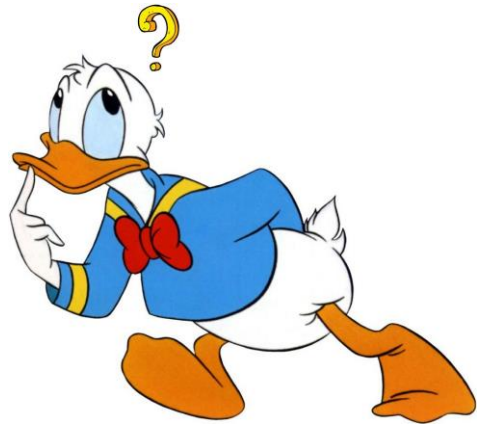
OSINT

Oper Source Intelligence

Benwick

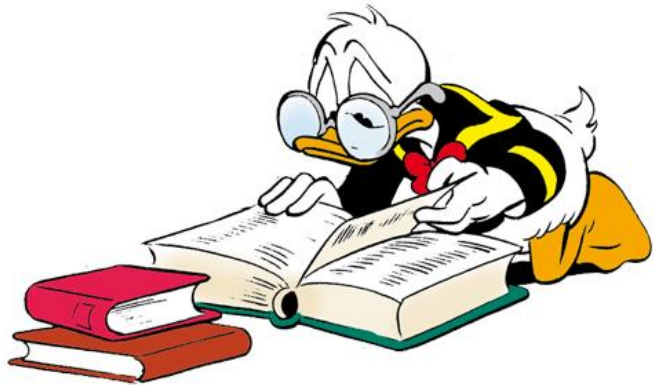
What is it?

- **Open-source intelligence** (**OSINT**) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources. It is not related to open-source software or public intelligence.
- Involves no classified information; no information that is subject to proprietary constraints (excluding copyright); and no information obtained from sensitive contacts, or through clandestine or covert means.
- OSINT is primarily used in national security, law enforcement, and business intelligence functions.



OSINT Categories

- **Media:** newspapers, magazines, radio, and television.
- **Internet:** online publications, blogs, discussion groups, citizen media (i.e. – cell phone videos, and user created content), YouTube, and other social media websites (i.e. – Facebook, Twitter, Instagram, etc.).
- **Public Government Data:** public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches.
- **Professional and Academic Publications**: journals, conferences, academic papers, and theses.
- **Commercial Data:** commercial imagery, financial and industrial assessments, and databases.
- **Grey literature:** technical reports, preprints, patents (brevetti), working papers, business documents, unpublished works, and newsletters.



Risks

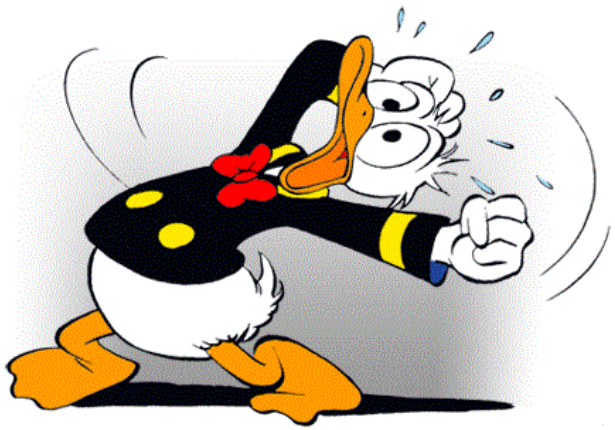
- A main hindrance to practical OSINT is the volume of information it has to deal with ("information explosion"). The amount of data being distributed increases at a rate that it becomes difficult to evaluate sources in intelligence analysis.
- Accredited journalists have some protection in asking questions, and researching for recognized media outlets. Even so, they can be imprisoned, even executed, for seeking out OSINT. Private individuals illegally collecting data for a foreign military or intelligence agency is considered espionage in most countries.
- You may need to go to the dark web.

Advantages

- OSINT is much less expensive compared to traditional information collecting tools and offers a potentially greater return on investment.
- Information can be legally and easily shared with anyone.
- Open sources are always available and constantly up to date on any topic.

Disadvantages

- Potential information overload and filtering insight from the “noise” can be difficult.
- Without valuable OSINT tools, finding and searching the right information can be a time-consuming activity.
- It requires a large amount of analytical work from humans in order to distinguish valid, verified information from false, misleading or simply inaccurate news and information.
- OSINT must be validated.

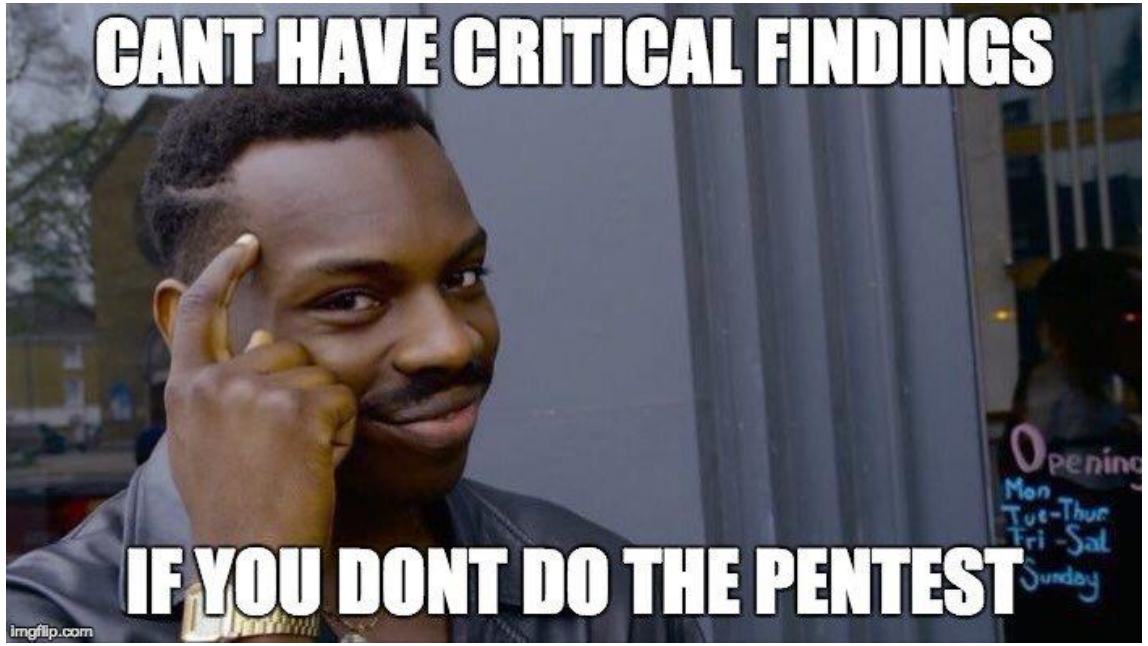


Where OSINT

OSINT can be used in various fields such as:

- Business
- Military
- National security
- Terrorism
- Law enforcement
- Finiding missing perople
- Organized crime
- Penetration testing
- PSYOP (Psychological operations) and fake news...

OSINT for PenTesting (aka: reconnaissance)



OSINT for PenTesting

Assume you are an ethical penetration tester working for a security company. Your boss walks over to your office and hands you a piece of paper. “I just got off the phone with the CEO of that company. He wants my best employee to Pen Test his company – that’s you. Our Legal Department will be sending you an email confirming we have all of the proper authorizations and insurance”. You nod, accepting the job. He leaves. You flip over the paper, a single word is written on the paper, “Syngress.” It’s a company you’ve never heard of before, and no other information is written on the paper.

What now?

- The more thoroughly you prepare for a task, the more likely you are to succeed.

OSINT for PenTesting

- Reconnaissance (information gathering), is the most important phases.
- The more time you spend collecting information on your target, the more likely you are to be successful in the later phases.

OSINT for PenTesting

Consider the following example: assume we have two different criminals who are planning to rob a bank. The first criminal buys a gun and runs into the first bank he finds yelling "HANDS UP! GIVE ME ALL YOUR MONEY!" It is not hard to imagine that the scene would be complete chaos and even if the bungling burglar managed to get away, it probably would not take long for the police to find him, arrest him, and send him to prison. Contrast this to nearly every Hollywood movie in existence today where criminals spend months planning, scheming, organizing, and reviewing details before the heist. They spend time getting weapons anonymously, planning escape routes, and reviewing schematics of the building. They visit the bank to determine the position of the security cameras, make note of the guards, and determine when the bank has the most money or is the most vulnerable. Clearly, the second criminal has the better chance of getting away with the money.

It should be obvious that the difference between these two examples is preparation and homework. Hacking and penetration testing is the same—you cannot just get an IP address and start running Metasploit (well you can, but you are probably not going to be very effective).

OSINT for PenTesting

So we have only the company name, how do we proceed?

Step 1 begins by conducting a thorough search of public information. The great thing about this phase is that in most cases, we can gather a significant amount of data without ever sending a single packet to the target.

Active reconnaissance includes interacting directly with the target. It is important to note that during this process, the target may record our IP address and log our activity.

Passive reconnaissance makes use of the vast amount of information available on the web. When we are conducting passive reconnaissance, we are not interacting directly with the target and as such, the target has no way of knowing, recording, or logging our activity.

OSINT for PenTesting

Oftentimes when conducting a penetration test, it is important to pay special attention to things like “News” or “Announcements.” Companies are often proud of their achievements and unintentionally leak useful information through these stories. Company mergers and acquisitions can also yield valuable data. Even the smoothest of acquisitions creates change and disarray in an organization. This transition period provides us with unique opportunities to take advantage of the change and confusion. Even if merger is old news or goes off without a hitch, the information still provides value by giving us additional targets. Merged or sibling companies provide a potential gateway into the organization.

OSINT for PenTesting

It is important to search and review any open job postings for the target company. Job postings often reveal very detailed information about the technology being used by an organization. Many times you will find specific hardware and software listed on the job opening.

For example, assume you come across a job requisition looking for a Network Administrator with Cisco ASA experience.

First, you can be certain that the company either uses, or is about to use, a Cisco ASA firewall. Second, depending on the size of the organization, you may be able to infer that the company does not have, or is about to lose, someone with knowledge of how to properly use and configure a Cisco ASA firewall. In either case, you have gained valuable knowledge about the technology in place.

Real case scenario (child abuse)

European Union Agency of Law Enforcement Cooperation, better known as Europol has been crowdsourcing parts of or heavily censored photographs, related to child abuse crimes in their “Stop Child Abuse – Trace an Object” campaign.

Europol received 10.000 contributions from the public.

Many followers of this campaign have helped by identifying objects and/or geolocating photographs.

Real case scenario (child abuse)

Europol
@Europol

Segui

This is a hotel room. Do U know which one? This info can help police solve a child sexual abuse case. Tell us on europol.europa.eu /stopchildabuse ...

05:00 - 11 ago 2017

Real case scenario (Trace objects)

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

Real case scenario (child abuse)

- Many followers of this campaign have helped by identifying objects and/or geolocating photographs. The location of a photograph in a hotel room was proved to be taken in a hotel on Mauritius within 48 hours after Europol shared the photograph on Twitter.
- 25 objects out of 70
- Were identified to one country or else to a reasonable number of countries of production and on 1 June 2018, more objects and countries of production were identified.

Real case scenario (child abuse)

Europol shared new images on their website and via Twitter on 15 October 2018. These were mostly of objects that need to be identified, but there were also a few photographs that were taken outside and are possible to geolocate because of recognizable landmarks.

Two of these photographs, taken from a roof of a building, show concrete buildings, and were presumably taken in an Asian city. According to Europol, a child was sexually abused in this city.

Real case scenario (child abuse)

Real case scenario (geolocation of photograph)

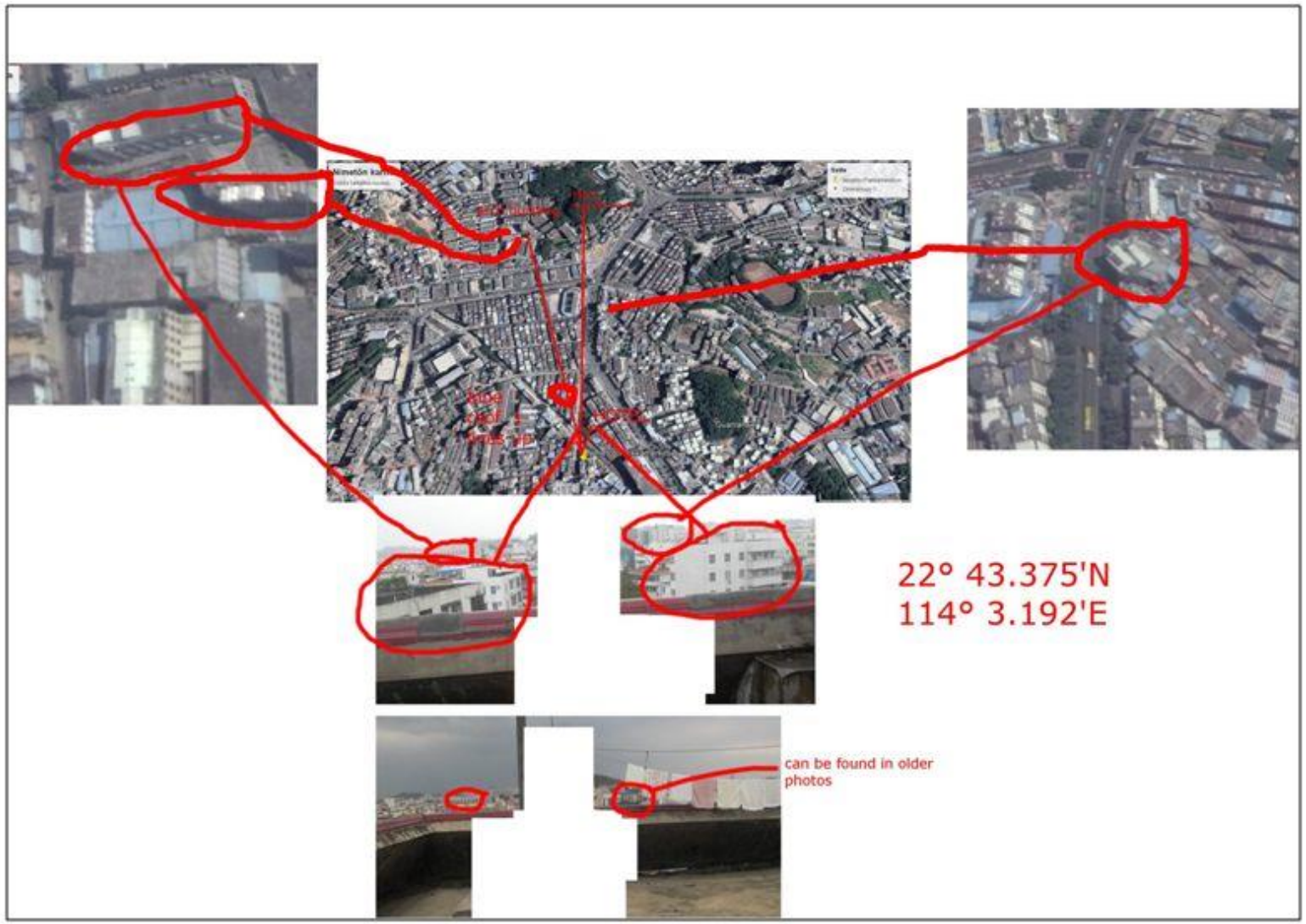
Many Twitter users responded to the tweet and mentioned a former Soviet Republic, Malaysia, Philippines or Indonesia as possible locations where the photographs were taken.

Twitter user “Bo” contacted Bellingcat and mentioned the architecture especially shows similarity to the city of Shenzhen in Southern China.

Sixteen days later, on 31 October 2018 Twitter user Olli Enne from Finland geolocated the exact location of the photographs in the Bao’an district of Shenzhen in Southern China.

Bellingcat: professional and citizen journalist investigations into war zones, human rights abuses, and the criminal underworld.

Real case scenario (geolocation of photograph)



Real case scenario (geolocation of photograph)

The geolocation of the photographs could not be immediately verified by Bellingcat, as it wasn’t easy to match the buildings of the photographs to the buildings visible in satellite imagery.

Yet due to street view on Baidu maps, a Chinese web mapping system, they were able to verify that Olli’s geolocation is a perfect match.

Baidu Maps is a desktop and mobile web mapping service application and technology provided by Baidu, offering satellite imagery, street maps, street view ("Panorama") and indoor view perspectives, as well as functions such as a route planner for traveling by foot, car, or with public transportation.

Real case scenario (geolocation of photograph)

Real case scenario (geolocation of photograph)

A Google Earth 3D view of the building the photographs were taken from in the same direction as in those photographs shows the same mountainscape.

Real case scenario (estimating photograph year)

Because the buildings in the photographs show more similarity to the same buildings in older street view captures, it is clear that the photographs were not taken recently.

A 2017 street view shows one of the buildings was even demolished and the buildings near to the location where the photographs were taken have brown netting.

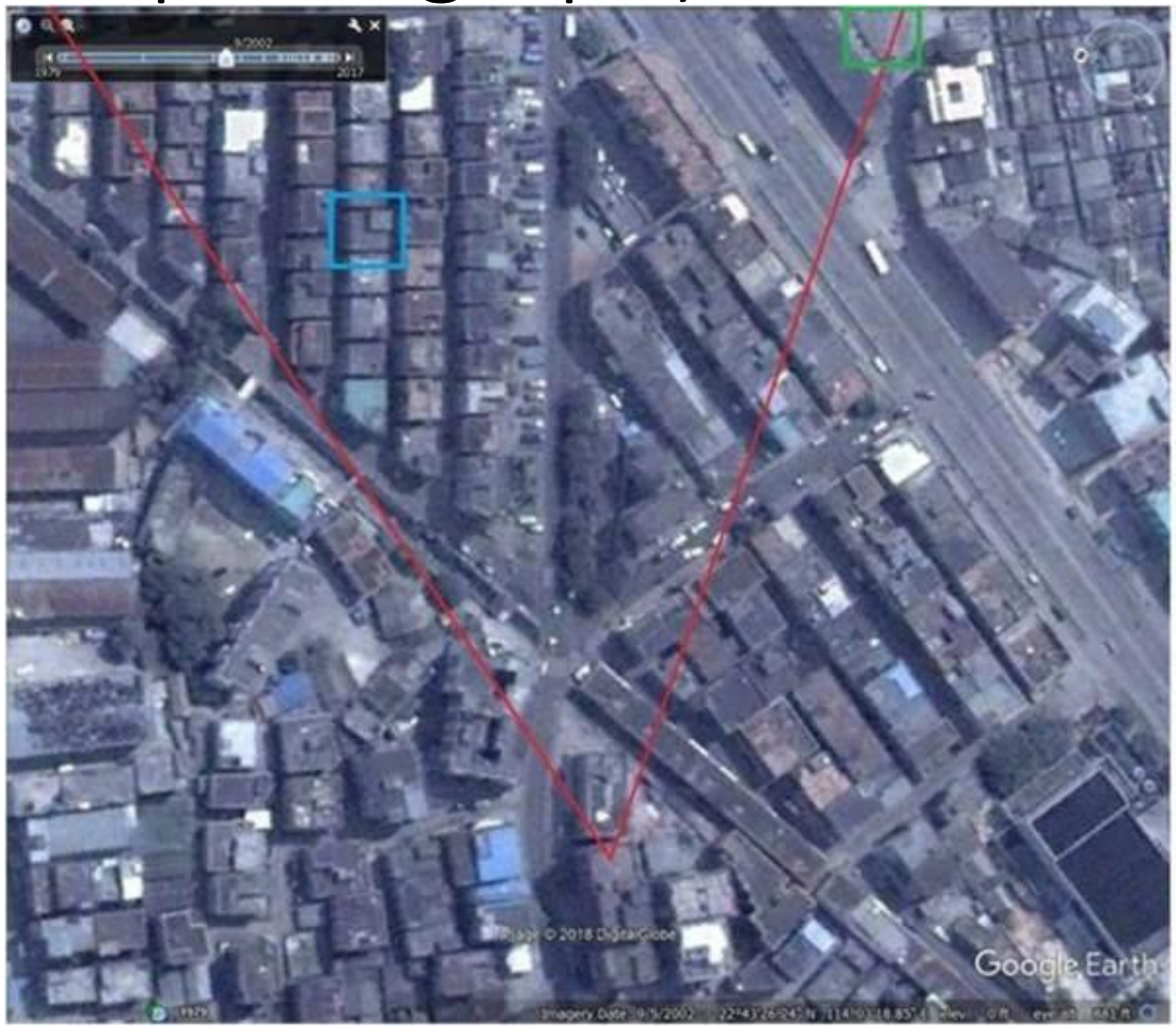
A 2014 street view capture shows GSM antennas on the white building on the left that are not visible in Europol's photographs. Recent street view shows many GSM antennas and satellite receivers in the area, while the Europol photographs only show one satellite receiver and three antennas.

Real case scenario (estimating photograph year)

Satellite imagery tells us the photographs had to have been taken after September 2002, as in the photographs one building clearly has a blue painted roof, which is not visible in satellite imagery from September 2002, but is visible in satellite imagery from February 2008. Also, two buildings visible slightly in the distance on the right side in one of the two photographs are not visible in 2002 satellite imagery, but are visible in 2008 satellite imagery.

The roughest estimation is between 2003 and 2013, so it’s most likely they were taken around 2008.

Real case scenario (geolocation of photograph)



Real case scenario (full description)

A complete description of the process of the cild abuse case can be found here: https://www.bellingcat.com/resources/case-studies/2018/11/08/europols-asian-city-child-abuse-photographs-geolocated/

Bogotà car bomb full investigation description: https://www.bellingcat.com/news/americas/2019/01/25/bogota-car-bomb-what-we-know/

Resources

Where can we find the information about a target?

With the advent of instant communications and rapid information transfer, a great deal of actionable and predictive intelligence can now be obtained from public, unclassified sources.

- Hidden public source (twitter + outlook)
- Facebook friend list from pictures like and comment.
- Hashtag search on Instagram and Twitter
- Google maps
- Street view etc. etc.

Resources

x0rz ha ritwittato

k @icommitfelonies · 10 gen

google is kind of a jerk lol

Traduci il Tweet

26 142 349

x0rz @x0rz · 16 dic 2018

Endless fake profile picture generation

Kevin Kelly @kevin2kelly

None of these faces are real. All made up by AIs. The end of photography as evidence. Research by @nvidia arxiv.org /pdf/1812.04948...

Traduci il Tweet

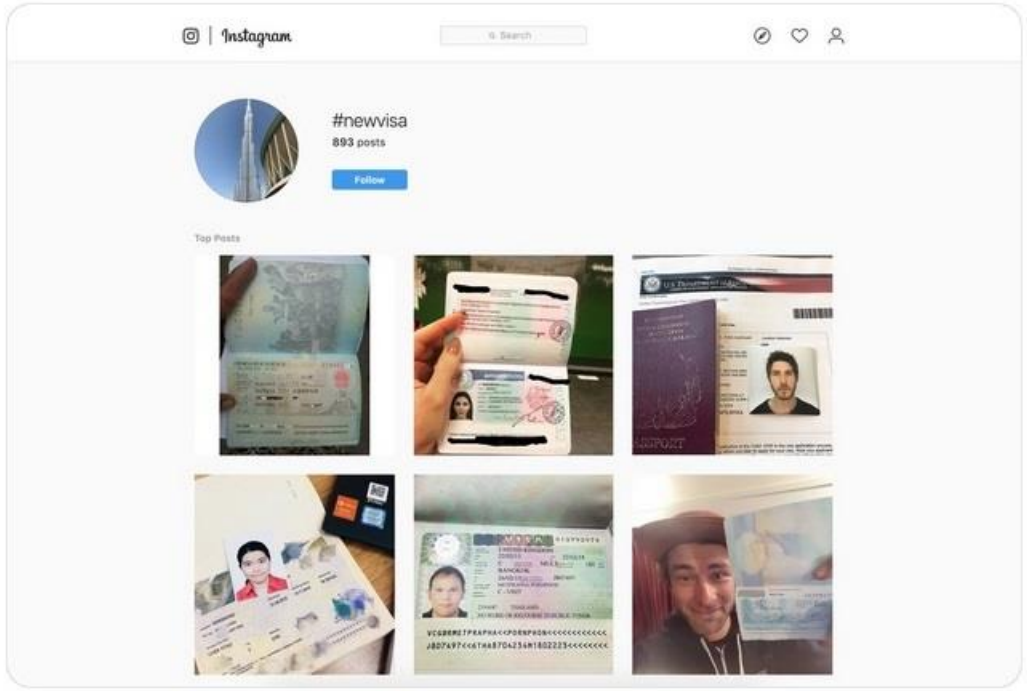
16 374 784

x0rz ha ritwittato

Zack Whittaker @zackwhittaker · 19 dic 2018

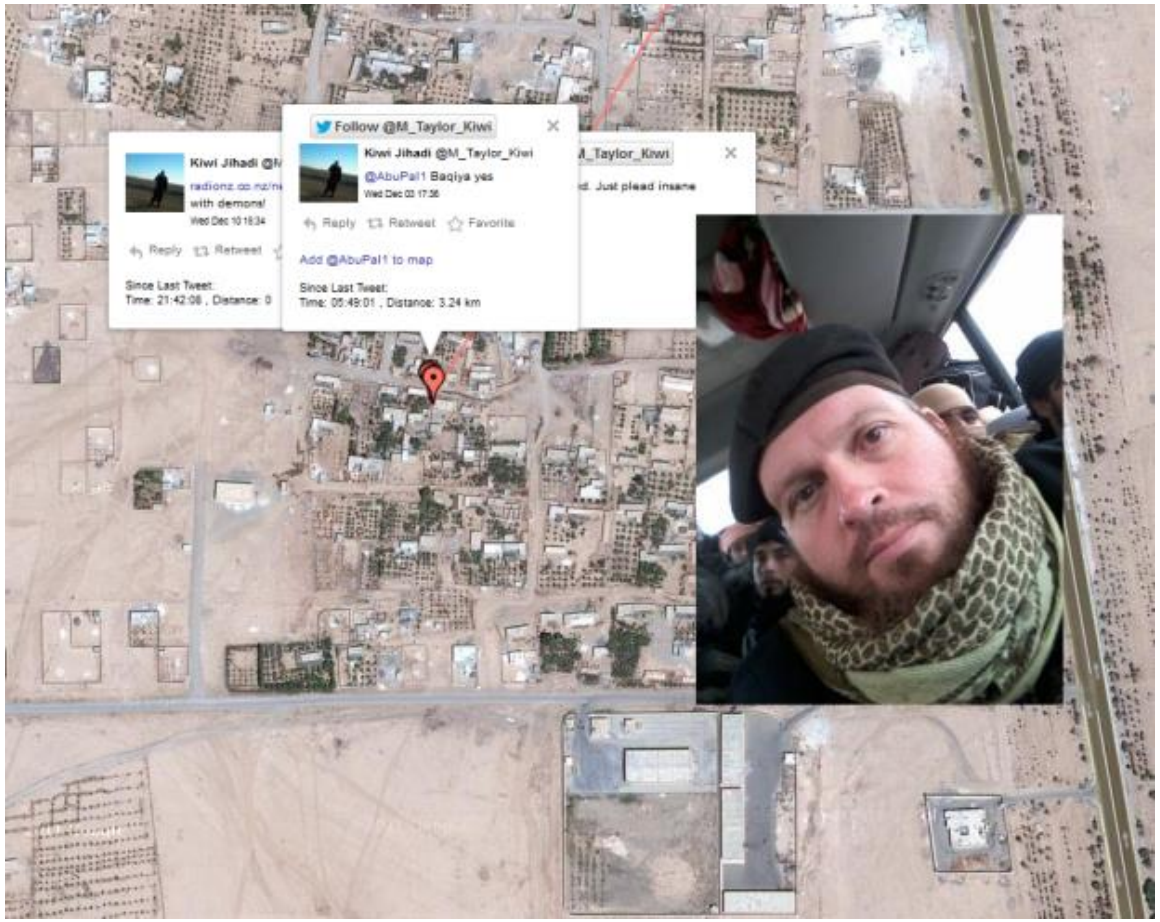
Ugh, people are posting their newly obtained visas on Instagram. (via @Cyber_War_News)

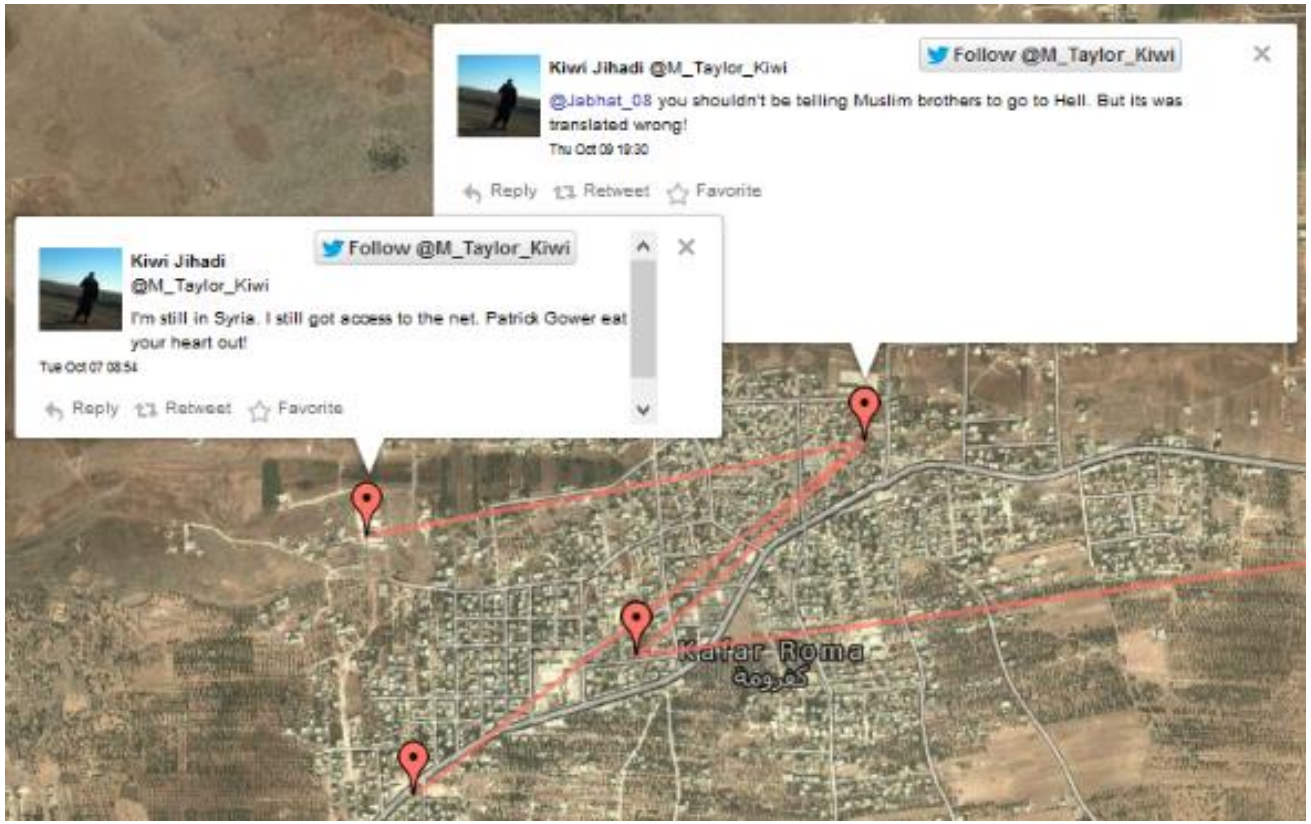
Traduci il Tweet



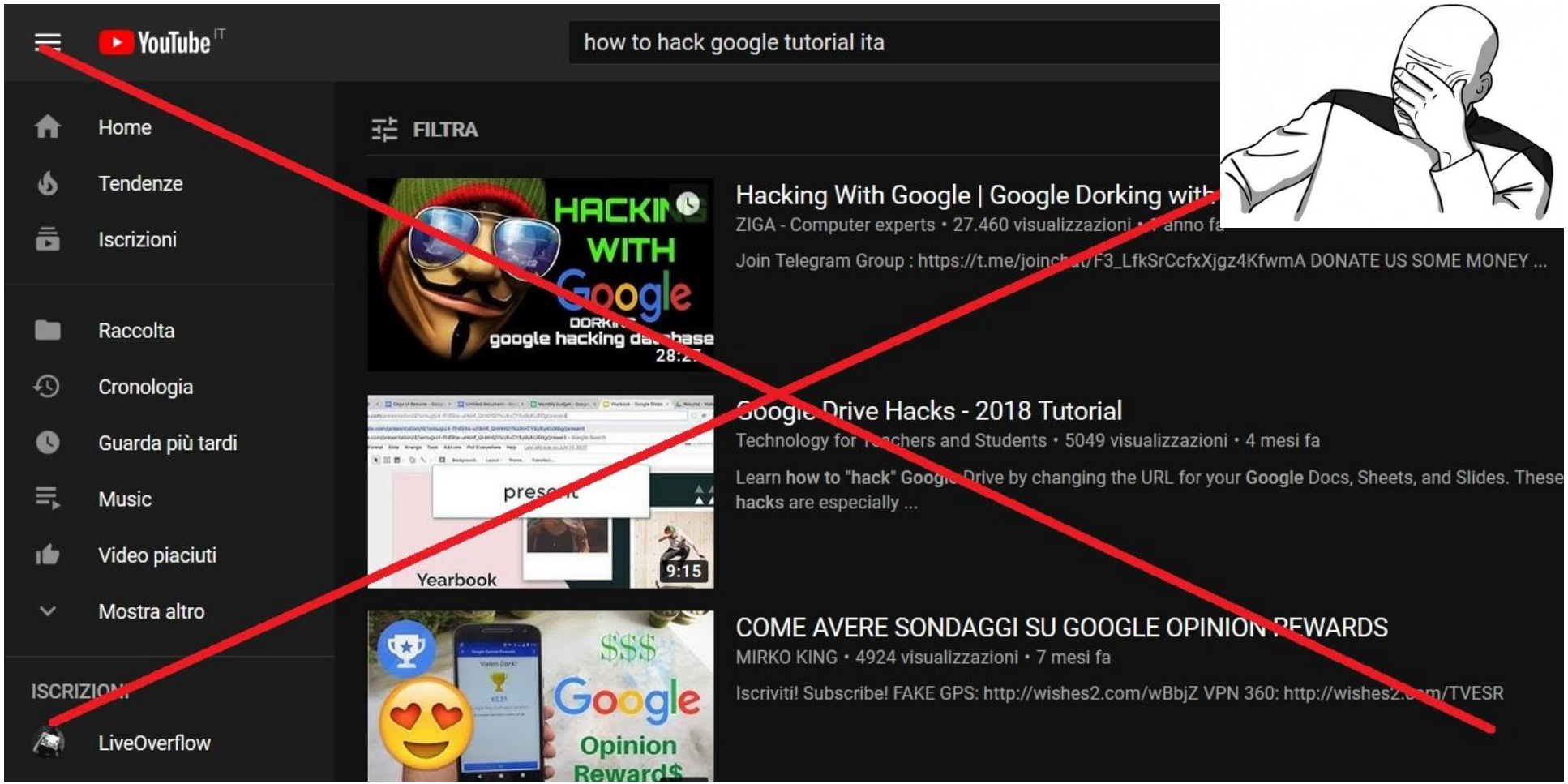
23 103 221

Sources


Follow @M_Taylor_Kiwi
Kiwi Jihadi @M_Taylor_Kiwi
@AbuPal1 Baqiya yes
Reply Retweet Favorite
Add @AbuPal1 to map
Since Last Tweet:
Time: 05:49:01 , Distance: 3.24 km


Kiwi Jihadi @M_Taylor_Kiwi
Follow @M_Taylor_Kiwi
@Jabhat_08 you shouldn't be telling Muslim brothers to go to Hell. But its was translated wrong!
Thu Oct 09 19:30
Reply Retweet Favorite
Kiwi Jihadi
@M_Taylor_Kiwi
Follow @M_Taylor_Kiwi
I'm still in Syria. I still got access to the net. Patrick Gower eat your heart out!
Tue Oct 07 08:54
Reply Retweet Favorite
Kafar Roma

Google Hacking



Google Hacking

Google hacking, also named **Google dorking**, is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.

Google hacking involves using advanced operators in the Google search engine to locate specific strings of text within search results.

Google Hacking (cheat sheet)

Advanced operators [edit]

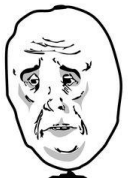
There are many similar advanced operators which can be used to exploit insecure websites:

Operator	Purpose	Mixes with Other Operators?	Can be used Alone?	Web	Images	Groups	News
intitle	Search page Title	yes	yes	yes	yes	yes	yes
allintitle[3]	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	specific files	yes|yes	yes	no	not really		
intext	Search text of page only	yes	yes	yes	yes	yes	yes
allintext	Search text of page only	really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	yes	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	yes	yes	not really
daterange	Search in date range	yes	yes	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	really	yes	no	yes	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes really	

The "link:" search operator that Google used to have, has been turned off by now (2017).[4]

Resources

Most of resource are for USA, couldn't find anything EU related.



- OSINT Framework.
- Google Hacking 101.
- Buscador OSINT (Operating System for OSINT).
- Trace Lab Resource (might me outdated).
- Investigation and Forensics toolbar.
- OSINT 101.
- OSINT 201.
- OSINT Resources 2019.
- Advanced OSINT tools.
- Advanced social media OSINT.
- Maltego.

OSINT is not only seaching informations with tools!

OSINT CTF

CTF about real missing person, all information gathered are sent to police!

- https://www.tracelabs.org/getinvolved/ctf/