#OSINT
Investigative visual research methods

Dataharvest 2021

By Ben Heubl
@BenHeubl

Overview

- Visual OSINT 101 for journalists
- Tracking extremism across Europe
- Ship tracking
- Other useful links

Visual OSINT 101 for journalists: What is it?

Analyzing video, photo and any other visual material

Visual OSINT

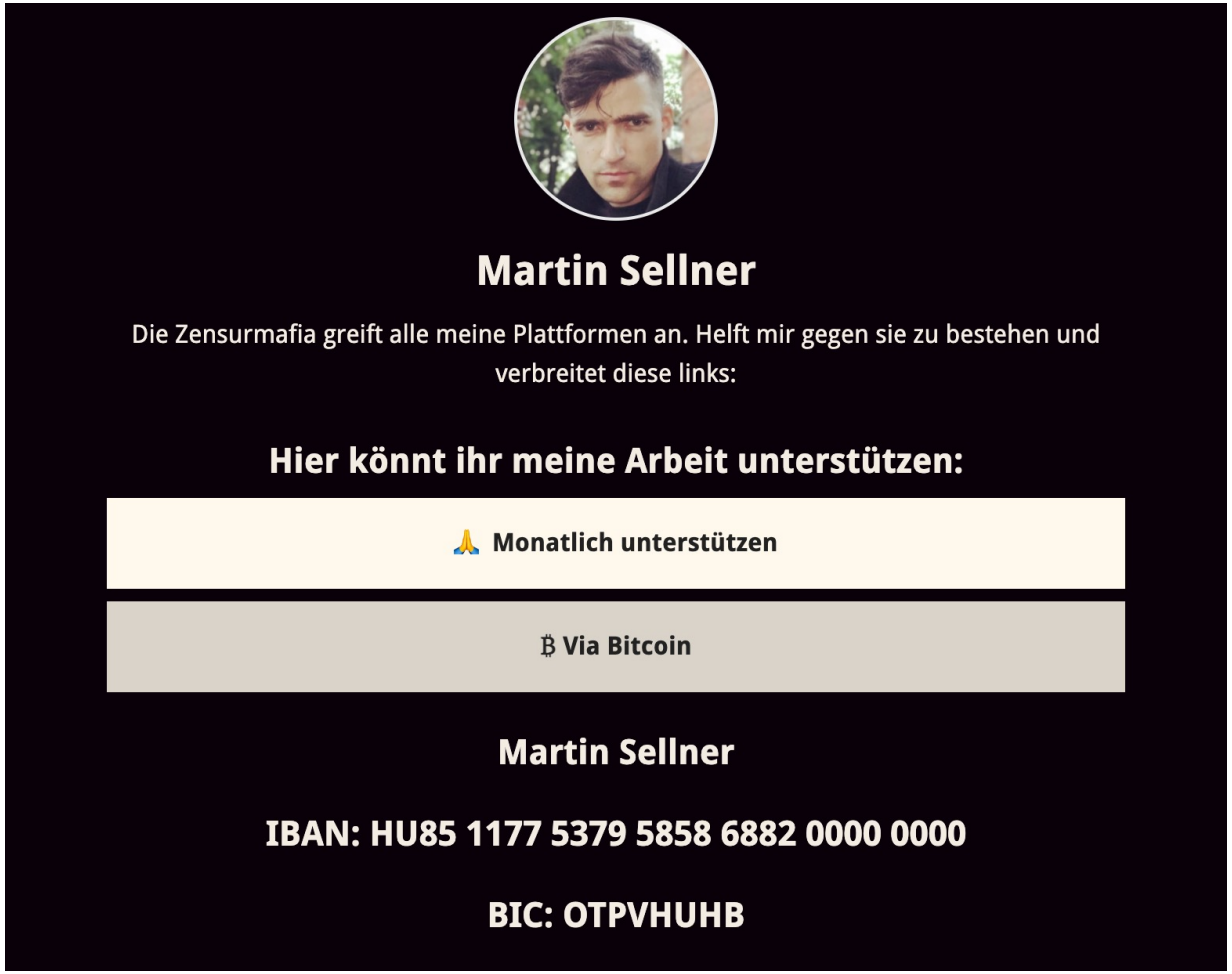
What kind of story do you want to tell with OSINT?

1. The Chain
2. The Pivot
3. The Pattern
4. Simple verification or ‘attestation’ story

Visual OSINT

The chain

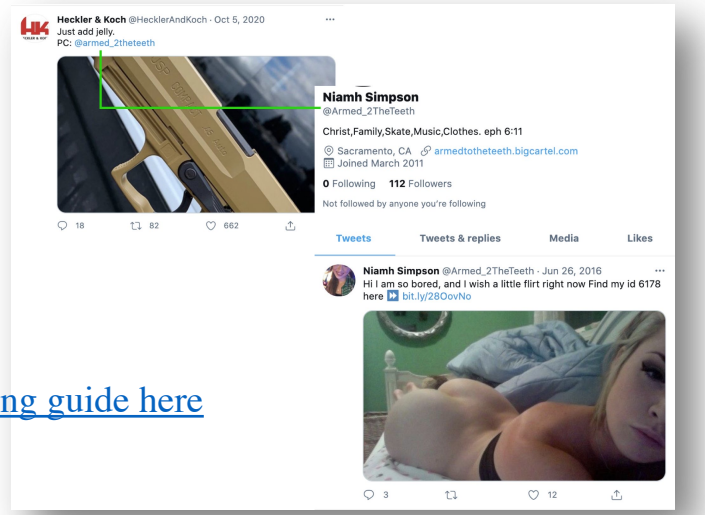
[Training guide here]

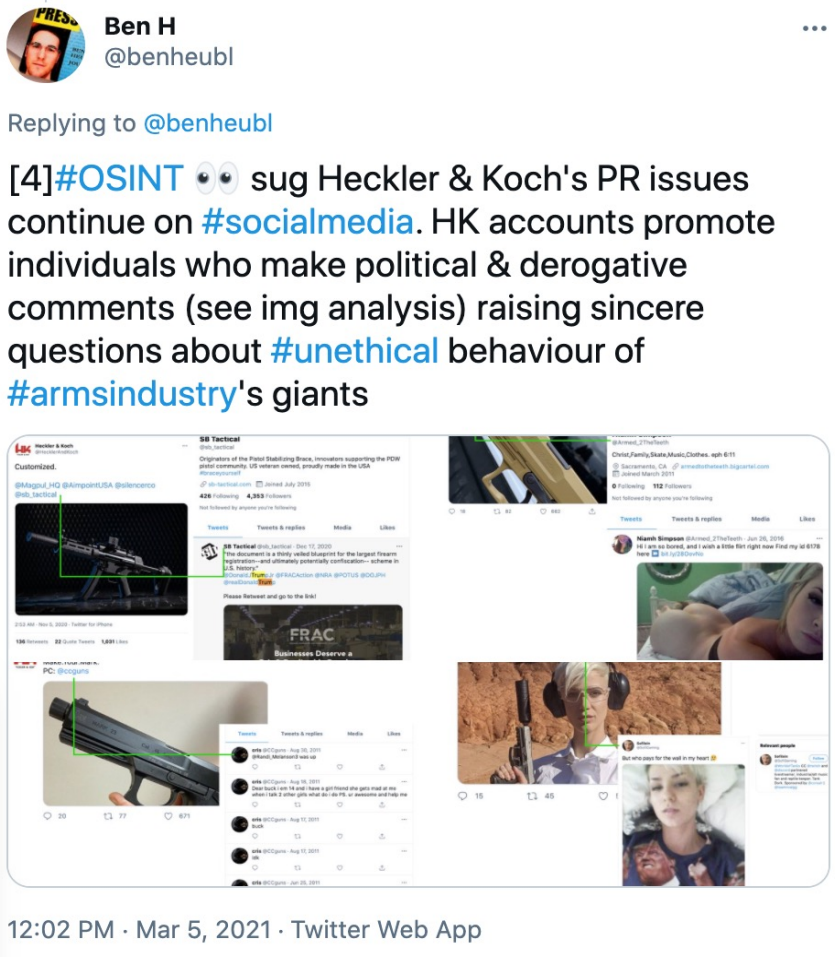


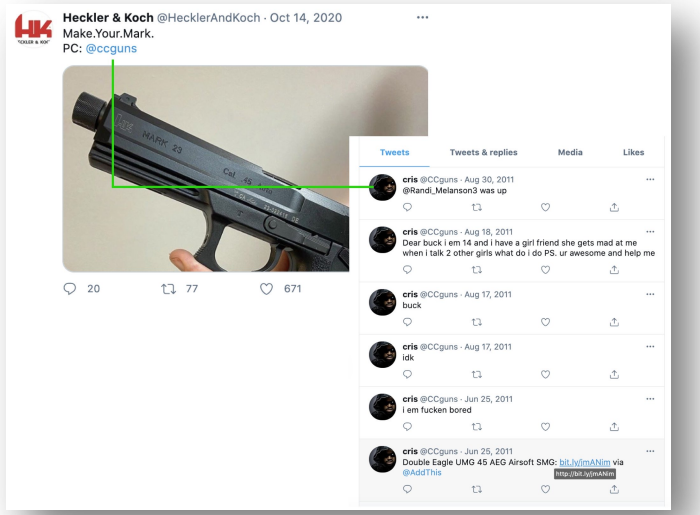
Visual OSINT

The Pivot

[Training guide here]



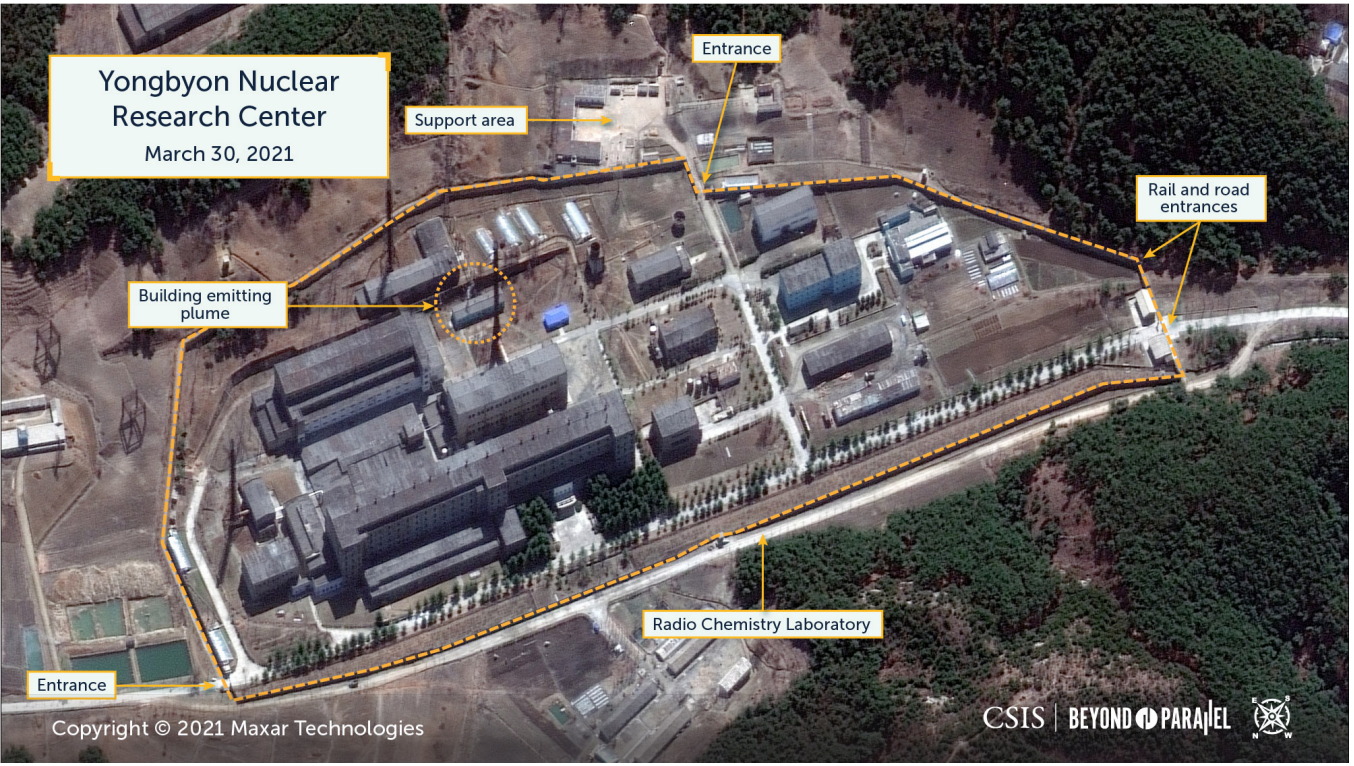




Visual OSINT

The Pivot

[NBC coverage here]



CSIS Korea Chair
@CSISKoreaChair

Satellite imagery of Yongbyon Nuclear Research Facility shows steam/smoke emanating from a small support building in the center of the facility, indicating that the building is being heated.

Snapshot by Joseph Bermudez & @VictorDCha / @CSIS

bit.ly/39q3mHi

Key points ⬇️

Reprocessing Activity at Yongbyon's Radiochemistry Laboratory? - Beyond ...
At the Yongyon Radiochemistry Laborat...
beyondparallel.csis.org

8:42 PM · Mar 30, 2021

14 1 Copy link to Tweet

Cargo ships from around the world are moving untracked in African waters, where the rise of a new fishing activity affects everything from local biodiversity to piracy.
By **Ben Heubl**

FISHING IN MURKY WATERS

THE VERACRUZ SHOULDN'T simply disappear. This is no small fishing boat but a 108m-long, 3,755 gross tonnage, refrigerated cargo ship built in 1977. Yet every time it crosses the sea border from Namibia to Angola it seems to do exactly that, as its operators switch off the automatic identification system (AIS) tracking signal. 'Going dark' contravenes the international treaty for Safety of Life At Sea (SOLAS) rules for ships like this of over 300 gross tonnage.

The Veracruz was repeatedly receiving catches from a local fishing vessel. This

owners take advantage of poor oversight in the region, where authorities appear powerless to control transshipping. Europe then benefits at the expense of some of the poorest nations in the world.

West Africa is a hotspot for what is known in the industry as illegal, unreported, and unregulated (IUU) fishing. The UN's Food and Agriculture Organization says IUU fishing and transshipping are tightly connected, and West African nations lose $2.3bn each year to it, according to *Frontiers in Marine Science* journal.

leave local fishers short of catch for the home market. Across West Africa, 37 species are now classed as 'threatened with extinction'. Between Angola and Mauritania, 14 others are nearly threatened, according to the International Union for the Conservation of Nature (IUCN).

Mapping the encounters

E&T's investigation followed several European cargo ships. Fisheries intelligence outfit Trygg Mat Tracking (TMT) provided us with a list of reefer vessels, some of them

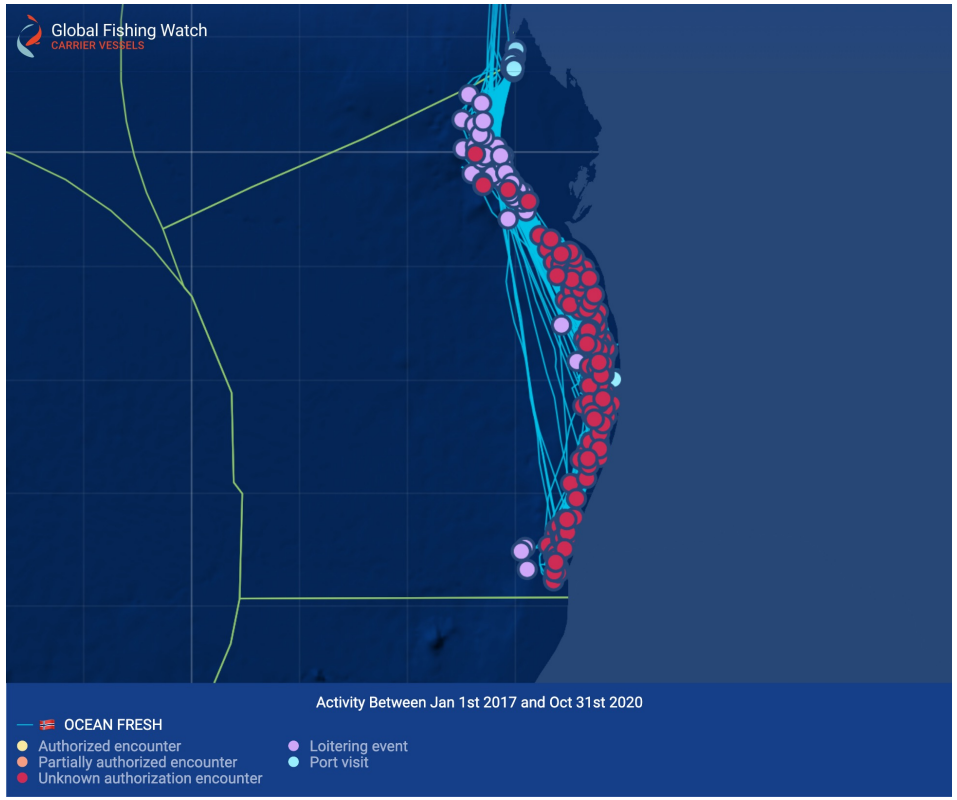
[Read the full investigation here]

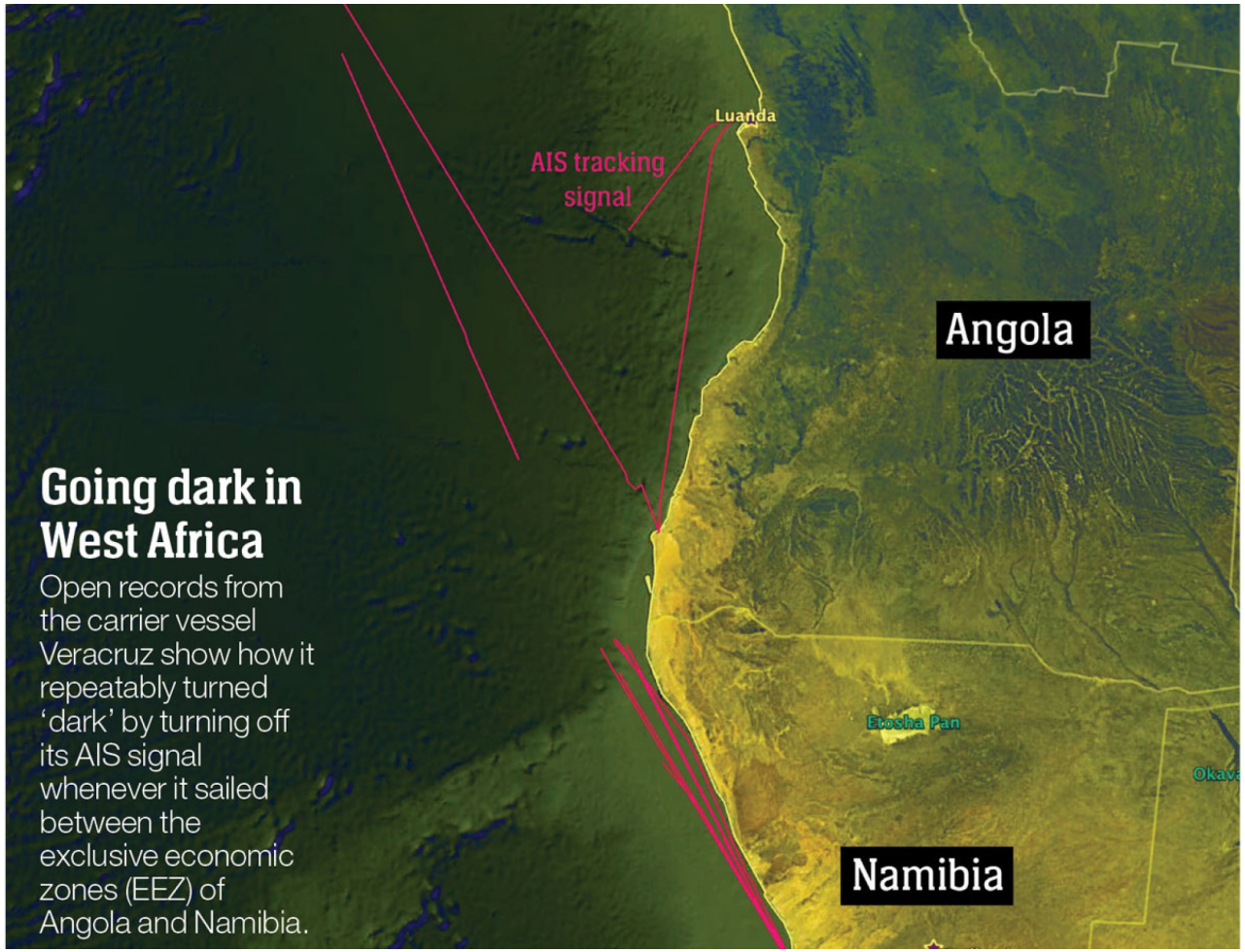
[Read the training post here]

Ship tracking

Case study:
Tracking illegal fish transshipments in West Africa

[Guide]





Case study:
Tracking illegal fish transshipments in West Africa

- Analyse fishing levels and possible illegal fishing activities

Global Fishing Watch
Carrier Vessel
(download AIS data)

Marinetraffic

Case: Ocean Fresh

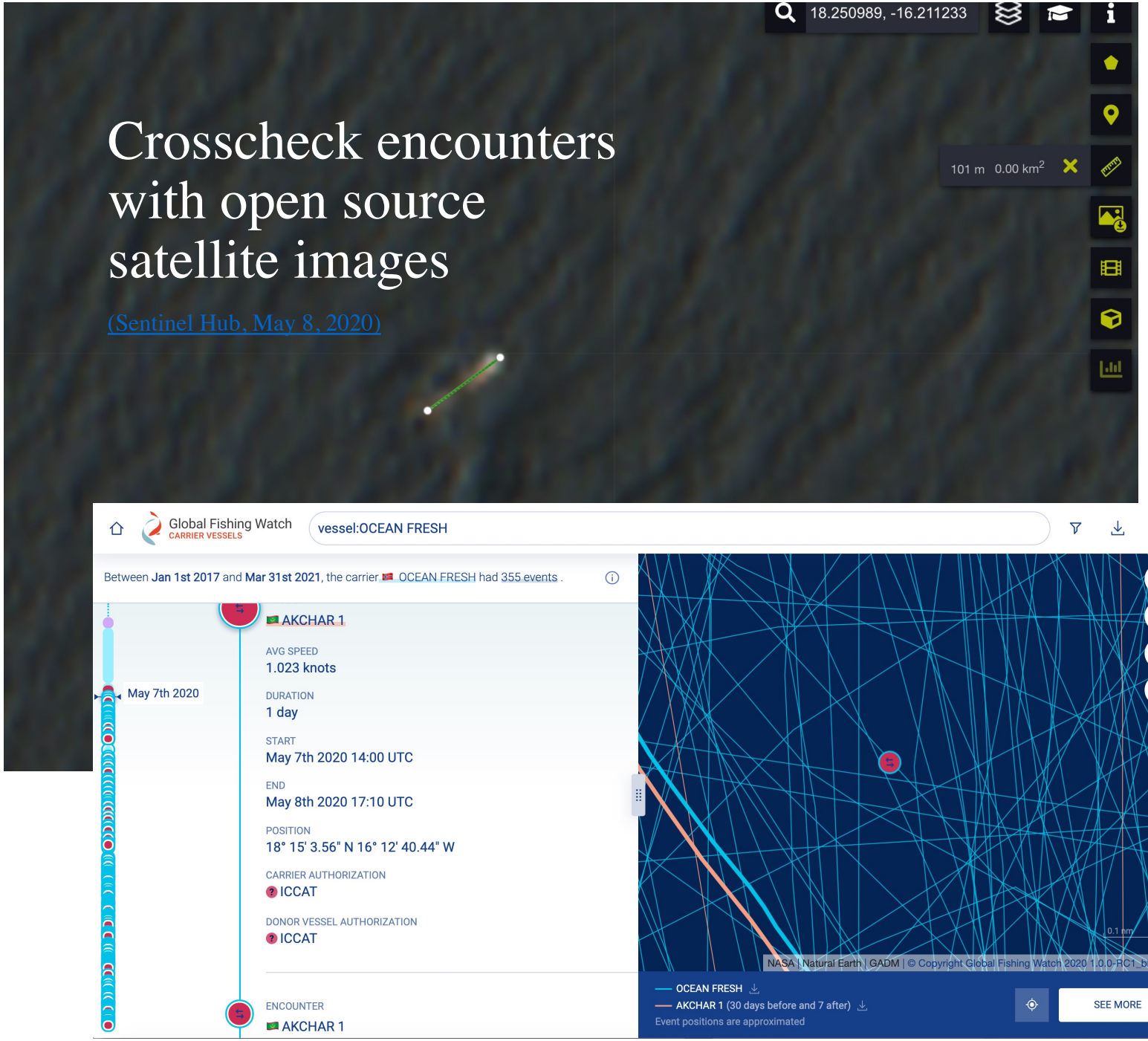
- IMO: 8301175
- Owner: Ocean Fresh Food Ltd
- Researching the crew

Case study:

- Analyse fishing levels and possible illegal fishing activities

Case: Ocean Fresh

- Crosscheck identity (s.a. length: 100m, use measurement tool)



Why tracking shipping vessels in the first place:

- Illegal acts (transshipping, sanction breaking behaviour, illegal fishing)
- Smuggling and human trafficking
- Maritime risk and piracy (dark fleets)
- Economic impact on coastal states

Methodology

- Start with vessel ID (IMO number)
- Access/analyse historical behaviour of vessel (AIS records)
- Check satellite images (open sat platfroms and commercial providers)
- Check human source: Check with people on the ground or on the ship (crew, via Linkedin etc.)

Technical approach

- Info/search on ship ID (MarineTraffic, VesselFinder etc)
- AIS: usually not open source but exceptions for IUU transshipments (Global Fishing Watch, FriendoftheSea, etc)
- Check satellite images (open images s.a. Sentinel 2 images or commercial Planet Labs or Maxar/DigitalGlobe)
- Search authorities or Wesbite to analyse crew on board

Ship-tracking tools/websites

- Inmarsat Ships Directory - Find contact details from a ship's name or number.
- Maritime Connector - Maritime jobs listings & search.
- Maritime Database - Lists and details of shipping-related businesses and ports of the world.
- Ship search & track:
  - VesselsFinder
  - MyShipTracking
  - Fleetmon
  - Shipfinder
  - Marine Traffic
  - CruiseMapper

Illegal rendezvous: Case study
Smoking gun with satellite images

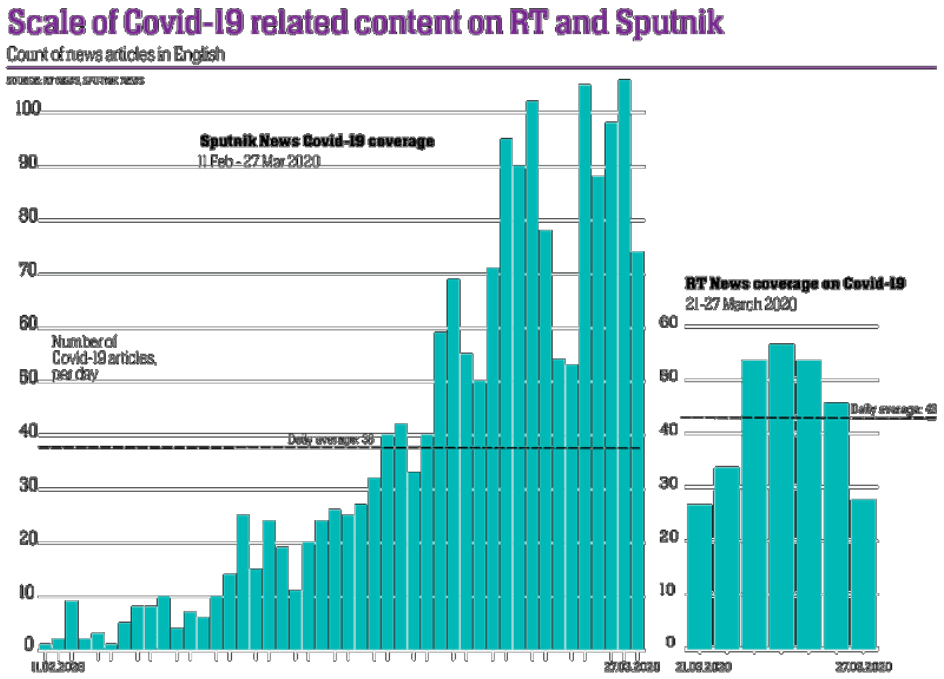
- Sentinel browser can reveal illegal meet-ups

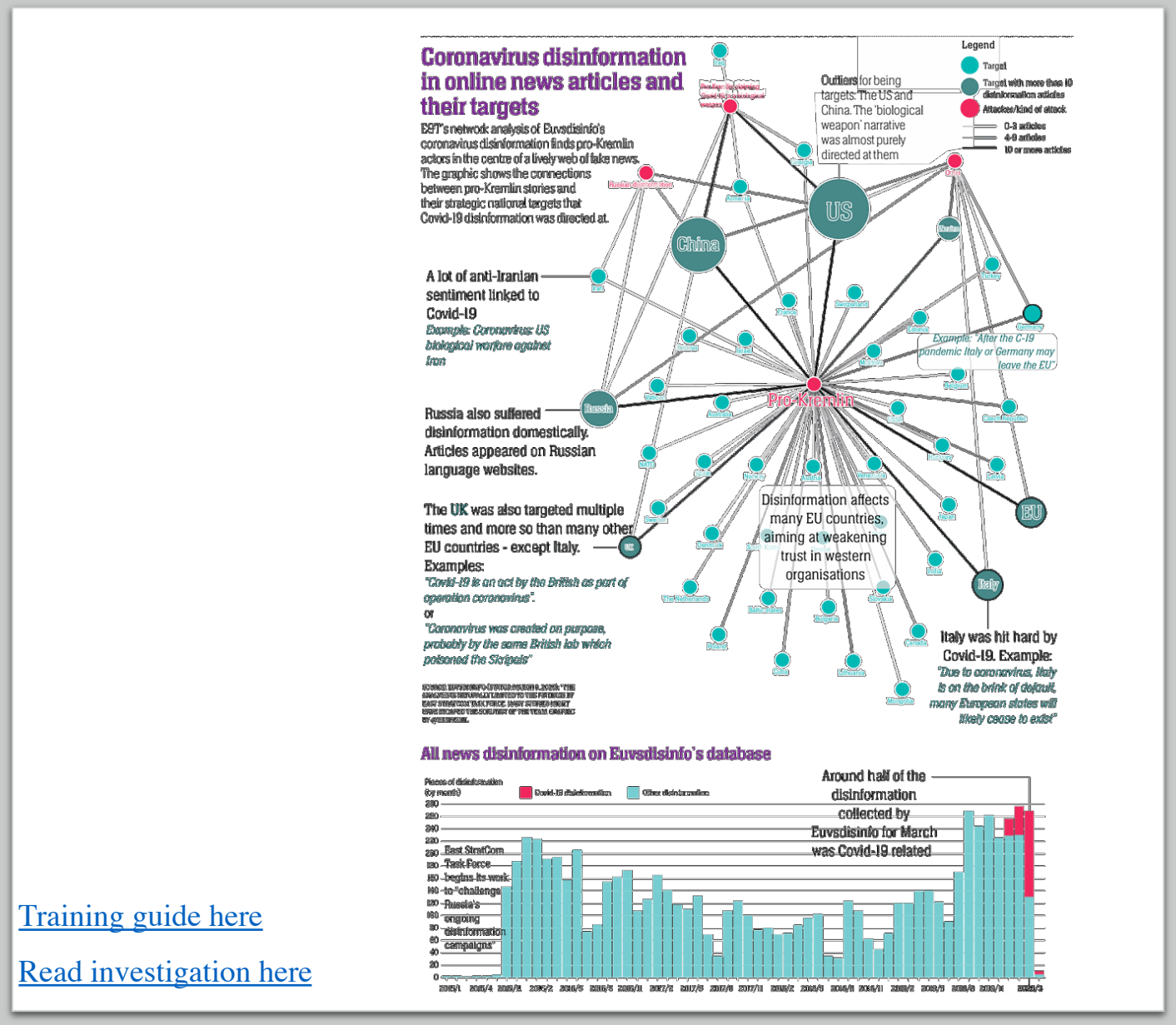
What to mind:

- Images might not be recorded (out of range)
- Not recorded on certain days (out of scope)
- Clouds that obscure the view

Visual OSINT

The pattern





[Training guide here]

[Read investigation here]

Visual OSINT 101 for journalists:

What story do you want to tell with OSINT findings

1. The Chain
2. The Pivot
3. The Pattern
4. Simple verification (or ‘attestation’)

Visual OSINT 101: Verification from footage

1. *State/collect/archive raw material*
2. *State obvious facts about the material*
3. *State assumptions*
4. *Verify assumptions with OSINT tools and methods*
5. *Getting stuck? Pivot/change previous assumptions*
6. *Present evidence*
7. *State caveats: any holes in the findings that leave a possibility of a different outcome?*
8. *Any other unexplored avenues?*

Visual verification: Geolocate from video

Typical mental approach:

1) Establish a list of facts (what can we see?)
2) Interpret: Establish hypothesis/questions
3) Define the country,
4) Define the region,
5) Test hypothesis (pivot if necessary)
6) Test and verify findings
7) Present/visualise findings

Visual verification: Geolocate from video

Technical approach:

- Panorama frame (stitched together via ai, your photo-editing program of choice)
- Reverse image search (Yandex etc.)
- Expert/local knowledge and details
- Background (mountains, colors etc.)

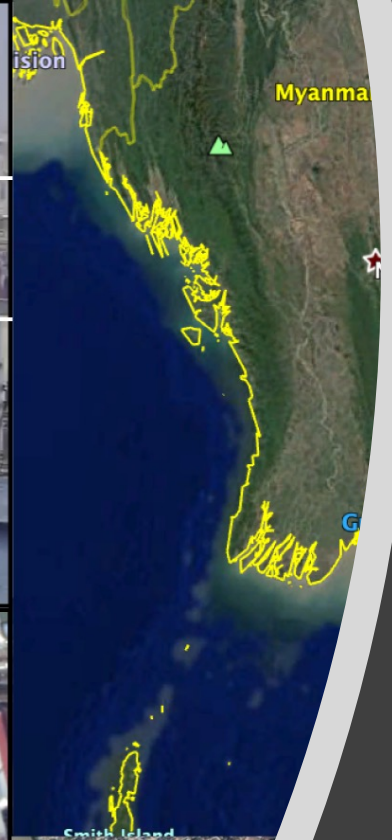
Visual verification: Geolocation

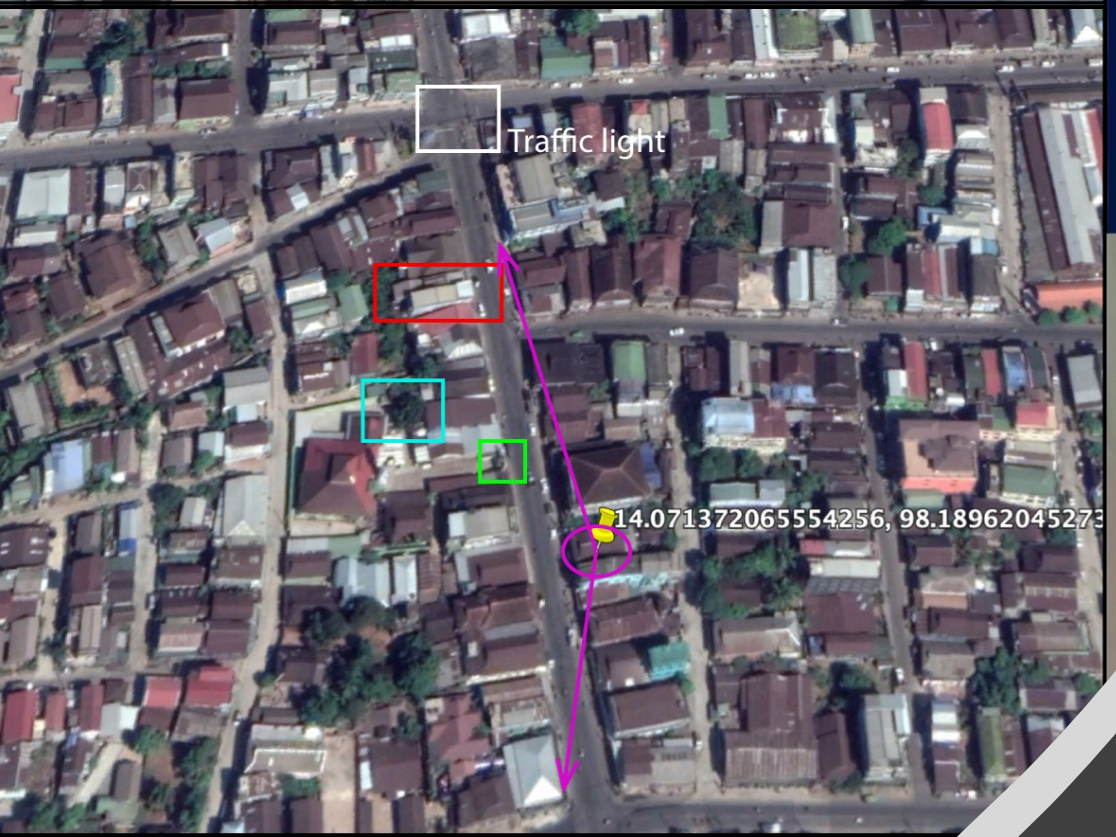
Supporting tools

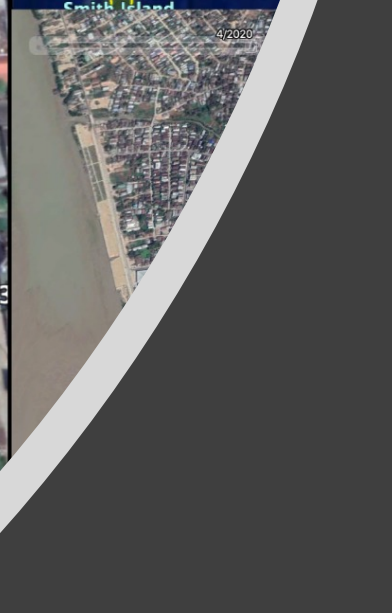
- Wikimappia (KML data export for Google Earth, another guide here)

http://wikimapia.org/ge.kml

- OpenStreetmap data (for QGIS)
- Google Earth Pro (with timeline slider, measurement tool, overlay)
- Google StreetView (to cross check results, if possible)







Visual verification: ‘Chronolocate’ from video

Case study

Visible ’facts’

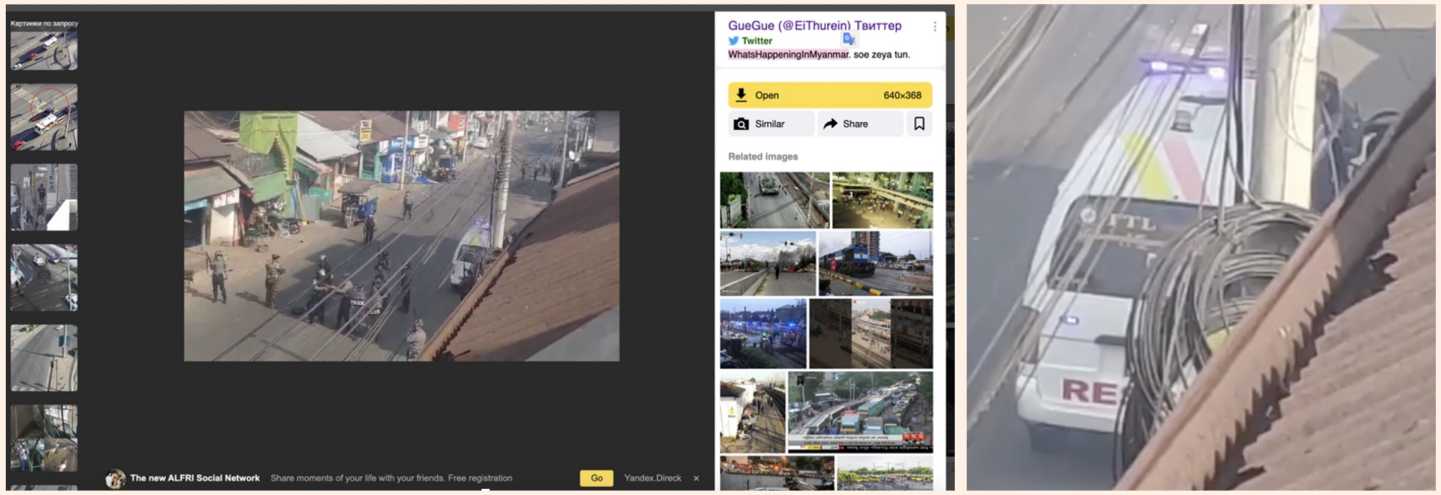
Videolink
Tutorial guide

- *Long street*
- *Armed men, in uniform*
- *Police car or ambulance*
- *A bank*
- *A car with a label*
- *A green gate of some kind*
- *No divider line on the street*
- *A traffic light down the road*
- *Shops opposite camera*
- *A tree in the background*

Shortcuts

- Reverse image search for police car on social media search: Yandex

We find new claims that this was shot in **Dawei, Myanmar**



Right: A screenshot test on Yandex, Left: The results, showing a post for the same video footage

=

Interpret:

Hypothesis/questions

- Police uniform indicate which country
- Bank branch indicate possible locations

Show 10 entries Search: dawei

No.	Branch Name	Address	Township	Division	Contact	Status
265	DAWEI	No.14, Neik Ban st, Myoetwin Qtr, Dawei.	Dawei	Taninthari	059-23467, 23468 23469	Close
270	DAWEI BRANCH (2)	No(857), Arzarni Rd, Kayatpyin Nort Qtr, DaWei, Tanintharyi Region.	Dawei	Tanintharyi	059-2021371, 2021374 2021375	Close

Showing 1 to 2 of 2 entries (filtered from 414 total entries) Previous Next

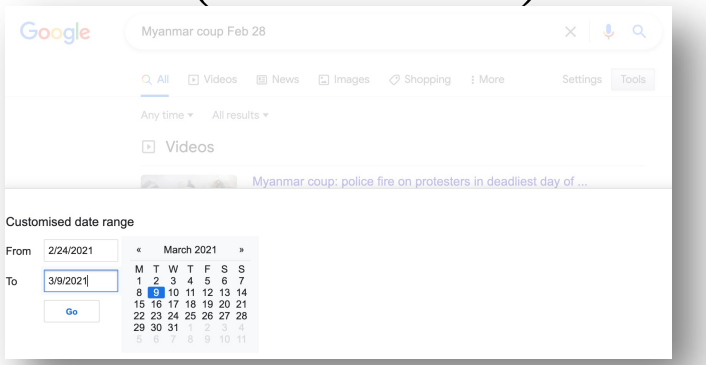
Results: Geolocation

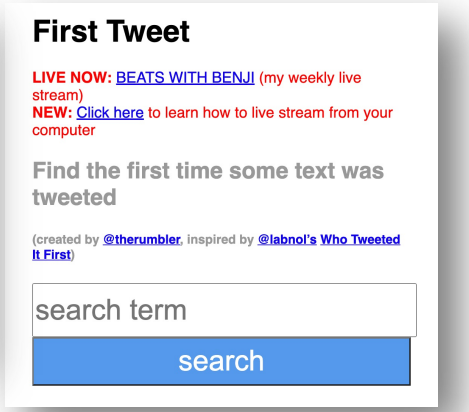
- The video was shot from a window facing first south-west and then north-west at the location of the coordinates 14.071372065554256, 98.18962045273268 in the city of Dawei, Myanmar, presumably in the morning of February 28 in 2021, between 8:00 and 9:30 am local time.

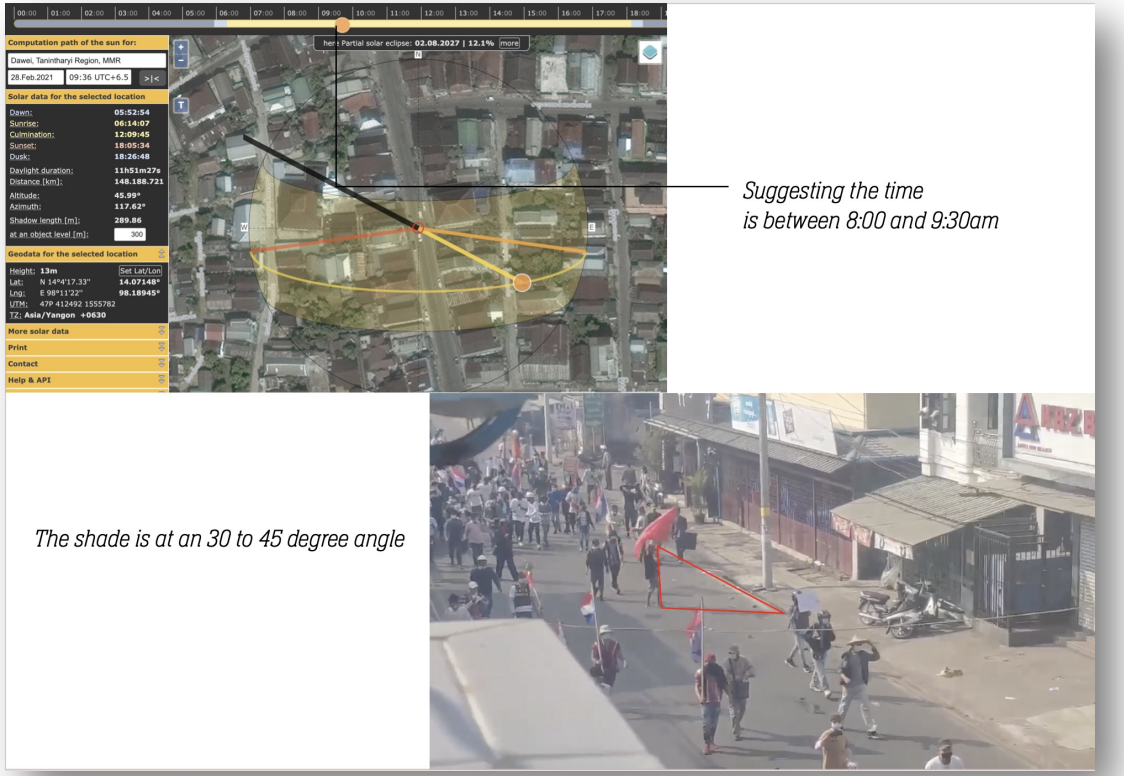
Results: Chrono-location

Tools:

- Suncalc.org
- Zoom.earth
- Search operator analysis (timeframe)







[Full blog post here](#)
[Additional guide (Bellingcat)](#)

Visual verification: Geolocate from video

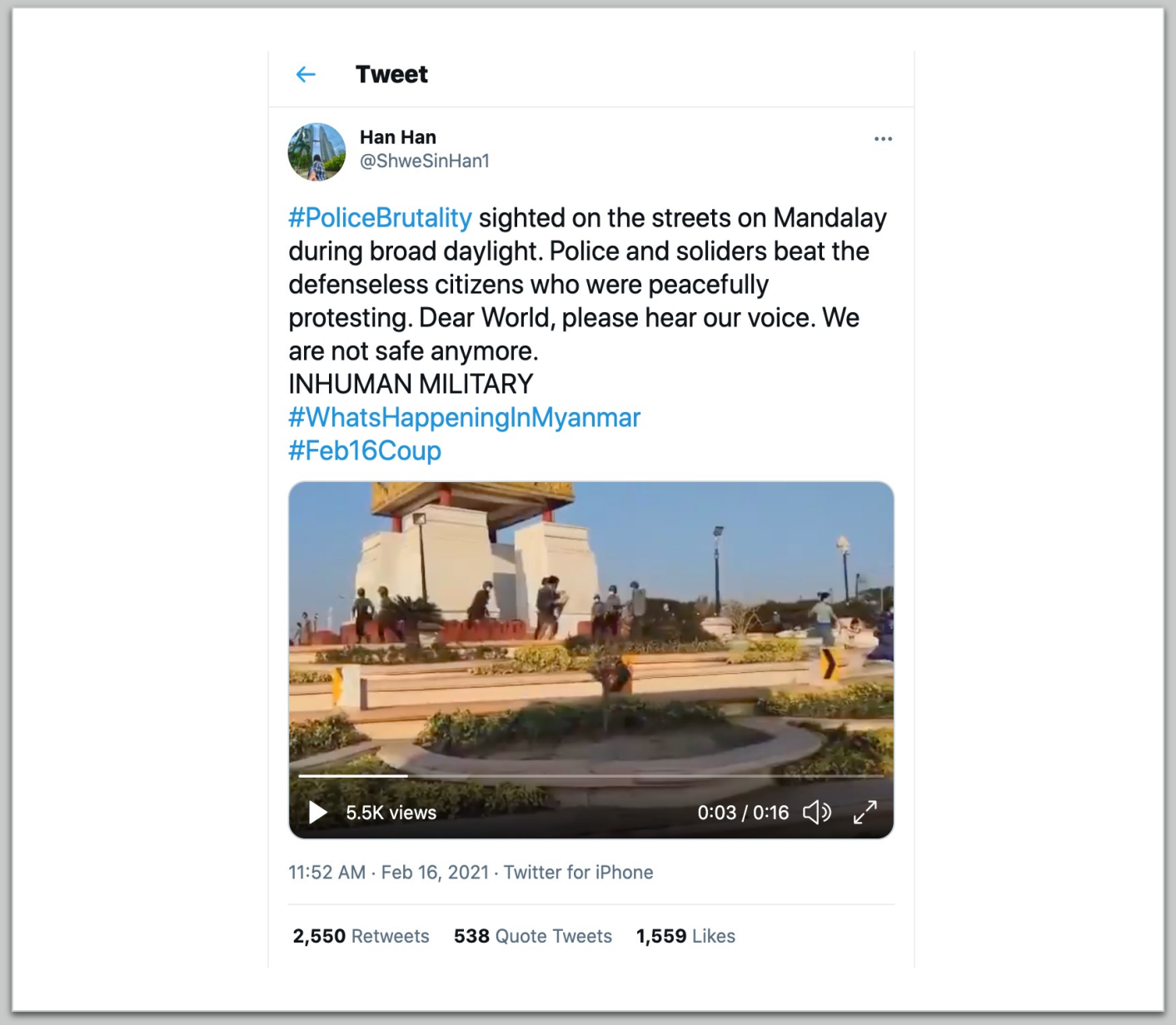
Video footage:

Twitter thread

Claims:

#PoliceBrutality sighted on the streets on Mandalay during broad daylight. Police and soliders beat the defenseless citizens who were peacefully protesting. Dear World, please hear our voice. We are not safe anymore. INHUMAN MILITARY #WhatsHappeningInMyanmar #Feb16Coup

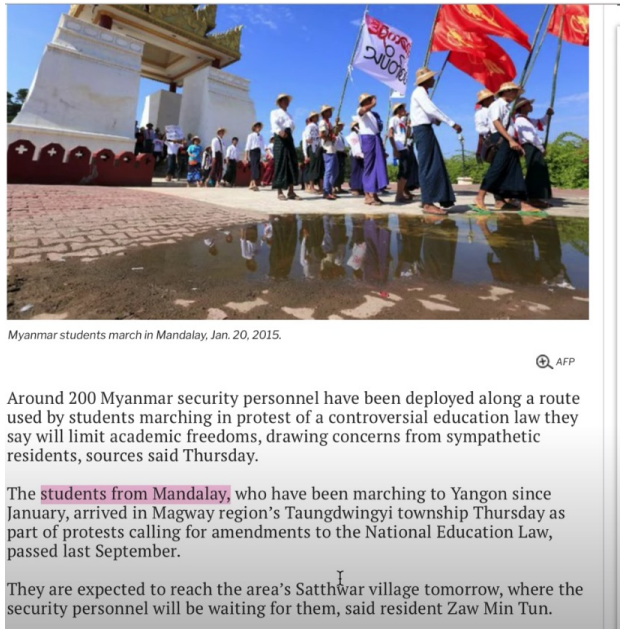
11:52 AM · Feb 16, 2021



Visual verification:

Reverse search
Bing Images - Can search part of an image by resizing on the fly.
CitizenEvidence - Google Images reverse search on YouTube thumbnails.
EagleEye - Find Instagram, FB and Twitter profiles using image recognition and reverse image search.
Google Images
Search by Image Browser extension to quickly reverse-search an image on 20+ search engines.
TinEye
Yandex Images

Reverse images search example



Myanmar students march in Mandalay, Jan. 20, 2015.

AFP

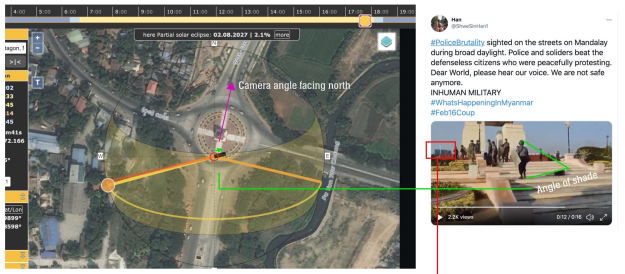
Around 200 Myanmar security personnel have been deployed along a route used by students marching in protest of a controversial education law they say will limit academic freedoms, drawing concerns from sympathetic residents, sources said Thursday.

The students from Mandalay, who have been marching to Yangon since January, arrived in Magway region's Taungdwingyi township Thursday as part of protests calling for amendments to the National Education Law, passed last September.

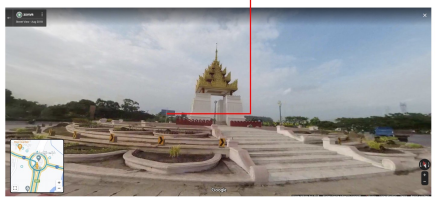
They are expected to reach the area's Satthwar village tomorrow, where the security personnel will be waiting for them, said resident Zaw Min Tun.

Use: Google Streetview (loc)

Same 'temple' where Myanmar students march in Mandalay on Jan. 20, 2015
rfa.org



Direction of camera:
From South to North
Location:
21.899447040310058,
96.08616062650096



Zoom.earth confirms cloudless weather

Visual verification: Geolocate from video

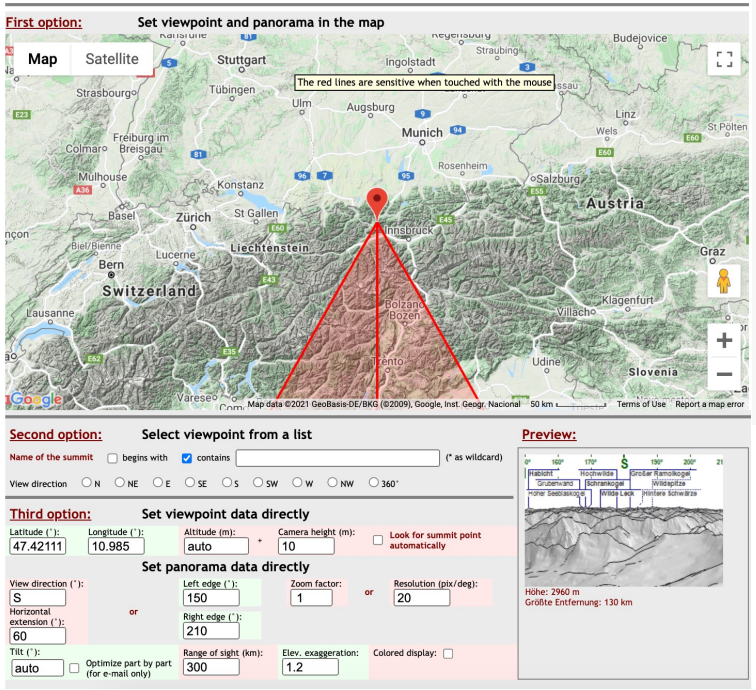
Mountain-ranges

Geo-tools for mountain range analysis:

- Peakfinder.org
- peakvisor.com
- Udeuschle.de/panoramas/makepanoramas_en.htm

Cross-check with:

- Sentinel browser 3D
- Google Earth 3D



Background: Mountains

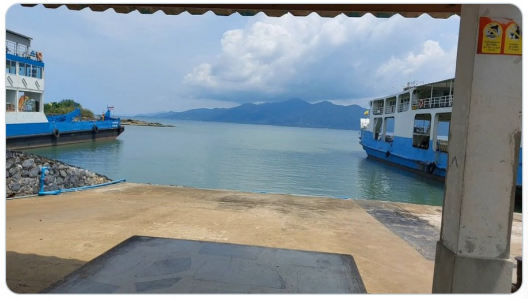
Lockpicking Pete | #BLM
@LockpickingPete

#Geolocation #Chronolocation #OSINTdojo

can you find out the following things?

📍 lat. long. of this location
⛵ can you travel with those ships? If so, can you find a schedule and prices?
🕰️ can you calculate the time with shadows?

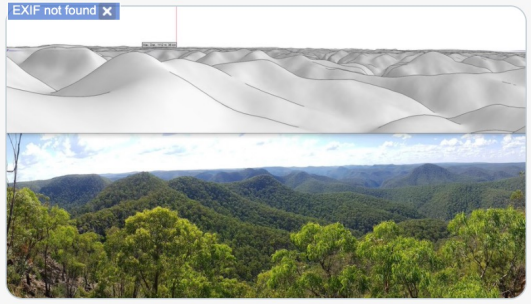
Answers please below the spoiler break!



ppim and OSINT Dojo

Nathan Ruser @Nrg8000 · Dec 27, 2020

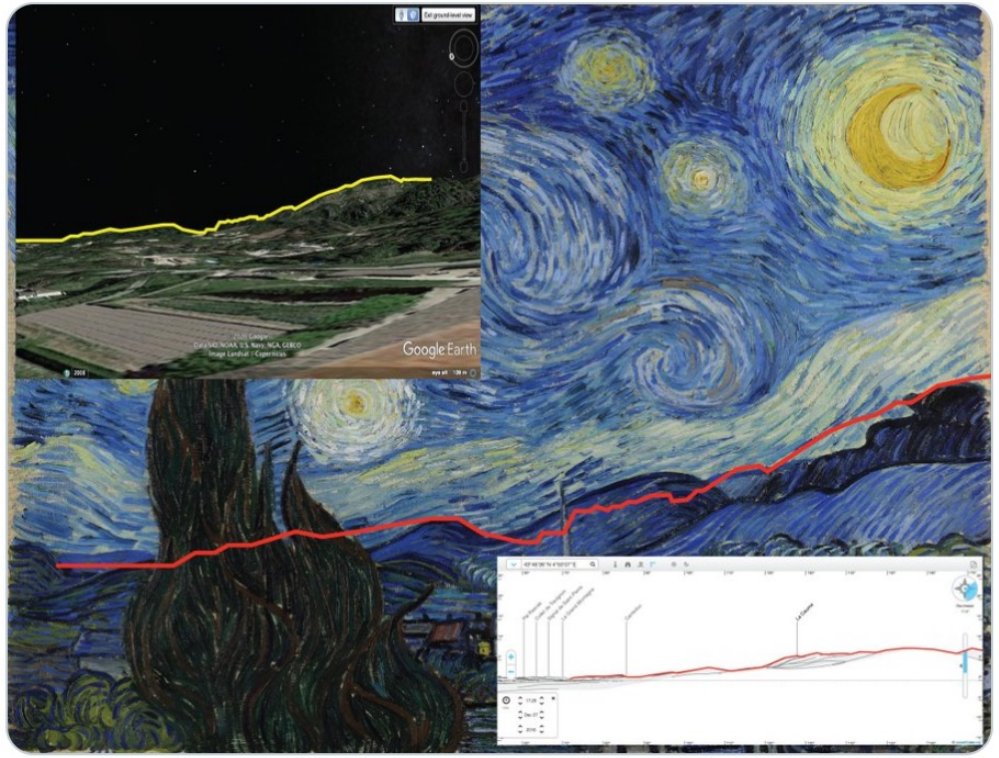
This tool, developed by Dr. Ulrich Deuschle and shared previously by @obretix is really very useful in geolocating photos with hills and mountains.
udeuschle.de/panoramas/make...
Here's it compared to a panorama from somewhere I visted today.
Bonus points if you can geolocate it...



5 23 109

Ben H
@benheubl

Researching classic landscapist art to train #OSINT works. Van Gogh's Starry Night allows to simulate the exact loc: Eastern view from bedroom window sketched in painter's asylum, 1st floor at Saint-Paul-de-Mausole (but painted 2nd-fl with SE view) - Peakfinder & GE, thx @Nrg8000



5:02 PM · Dec 29, 2020 · Twitter Web App

Visual verification: Geolocate from video

Mountain range

Missing hiker example:

NYT

Mr. Compean sent an SOS message and this photo to a friend.

Los Angeles County Sheriff's Department

Visual verification: Geolocate from video

Visual verification: Geolocate from video

Video:

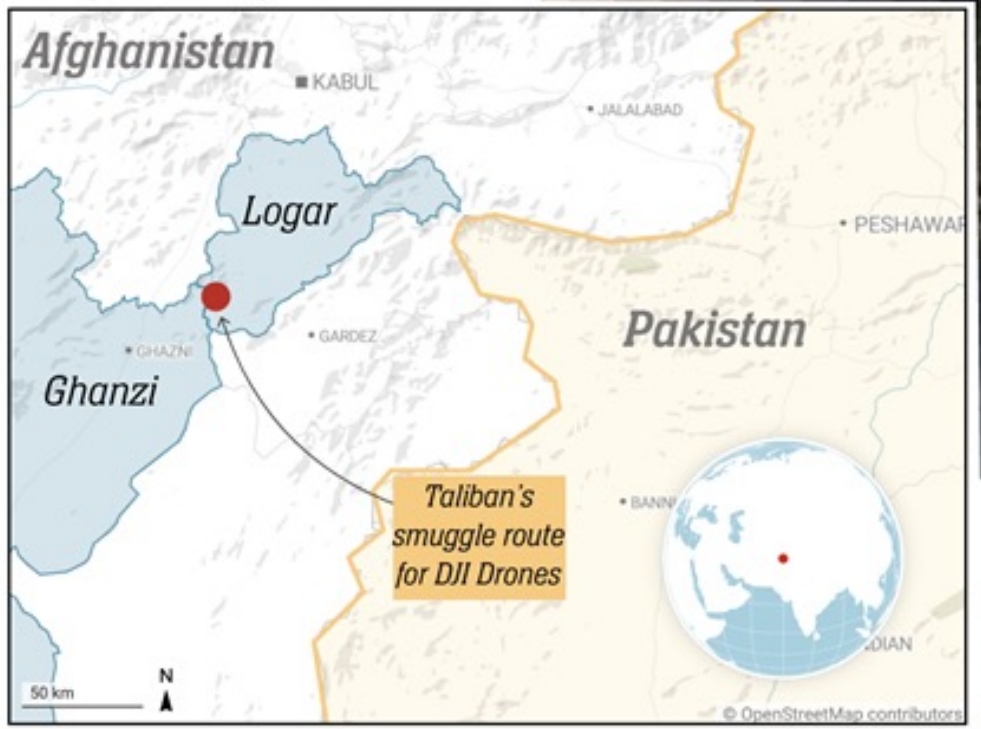
Local knowledge on peculiarities can play a huge role in narrowing down where a video was filmed

Full investigation here

Consumer drone warfare continues in Afghanistan

Open-source intelligence from video material offers clues where a video by Taliban soldiers and their DJI drone was filmed.

"There is no other way to bring drones into Afghanistan", E&T is told. Afghanistan border police at Kabul international airport is instructed to seize any drone they see. Smuggling via land from Pakistan - its border is less than 100km further east - seems the most plausible option.



2020:

The location of the filmed scene is most likely located between the Afghan province of Logar and Ghazni in the east of the country. The border to Pakistan is not far. It's possible the DJI drone and its equipment came from there.

[Full investigation here]

Source/data/intelligence: Twitter; Google Earth, @bsarwary; @CYSECATOM; Analysis: @BenHeubl

Visual verification: Video/images & Exif-data

Exchangeable Image File Format

[Exiftool]
Exif Viewer ([Firefox]/[Chrome])
[FotoForensics]
[Ghiro]
[Jeffrey's Image Metadata Viewer]
[mat2]
[mat2-web]
[StolenCameraFinder]

[EXIF data on Flicker is extensive]

Visual verification: Video/images & Exif-data

Case-study:

A video from a YouTube channel reveals EXIF data of the people involved in the **trophy hunting** business shown on camera.

Full investigation here

Mattw's tool on YouTube metadata reveals relevant tags of hunters otherwise would have remained hidden.

Warning: EXIF data can be manipulated, so has to be verified.


```
    "tags": [
        "African",
        "Safari",
        "Hunting",
        "Lion",
        "Buffalo",
        "Leopard",
        "Elephant",
        "Rhino",
        "Crocodile",
        "Hippo",
        "Cape Buffalo",
        "African Safari",
        "African Safari Films",
        "Safari Video",
        "Lew Harris Safaris",
        "Johan Calitz",
        "Wintershoek",
        "Johnny Vivier",
        "Ivan Carter",
        "Craig Boddington",
        "Hunting South Africa",
        "Hunting Africa",
        "African sun productions",
        "Mark Sullivan",
        "Tanzania",
        "Zimbabwe",
        "Zambia",
        "Namibia",
        "Botswana",
        "Mozambique",
        "Kruger Park",
        "Sable",
        "Roan",
        "Dangerous Game",
        "Plainsgame",
        "Hunting video"
    ],
```

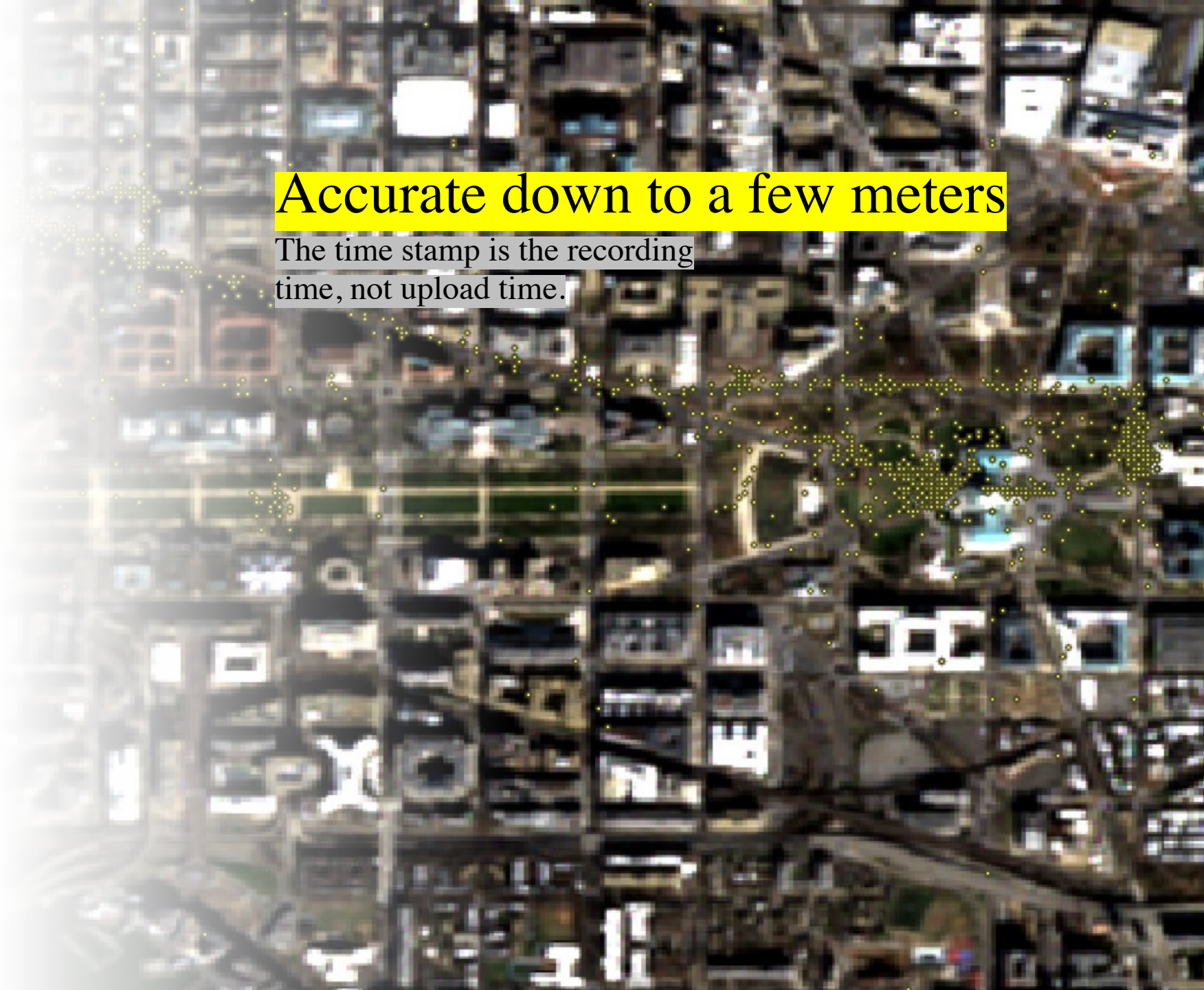
Visual verification: Video/images & Exif-data

Case-study: Capitol Hill riots

- Meta data lat longs of videos uploaded Parler between certain times

- Tools: QGIS, Google Earth

Read full post here



Visual verification: Geolocation – Using people to lead us to ‘secret location’

Casestudy: “Where Boeing tested/displayed its Loyal Wingman aircraft”

Loyal Wingman (image) debut in ‘secret location’ somewhere in Queensland , AUS, but not specific.

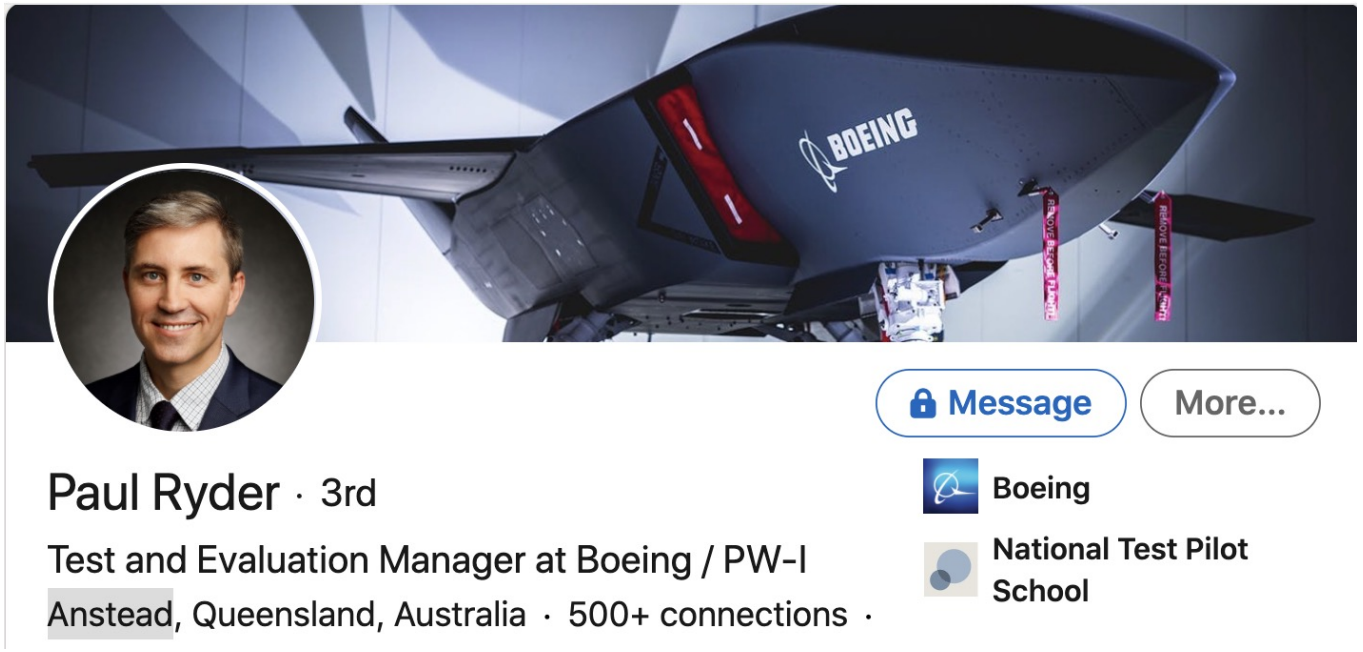
But where?

[Full investigation here]

The weakest link:

Humans

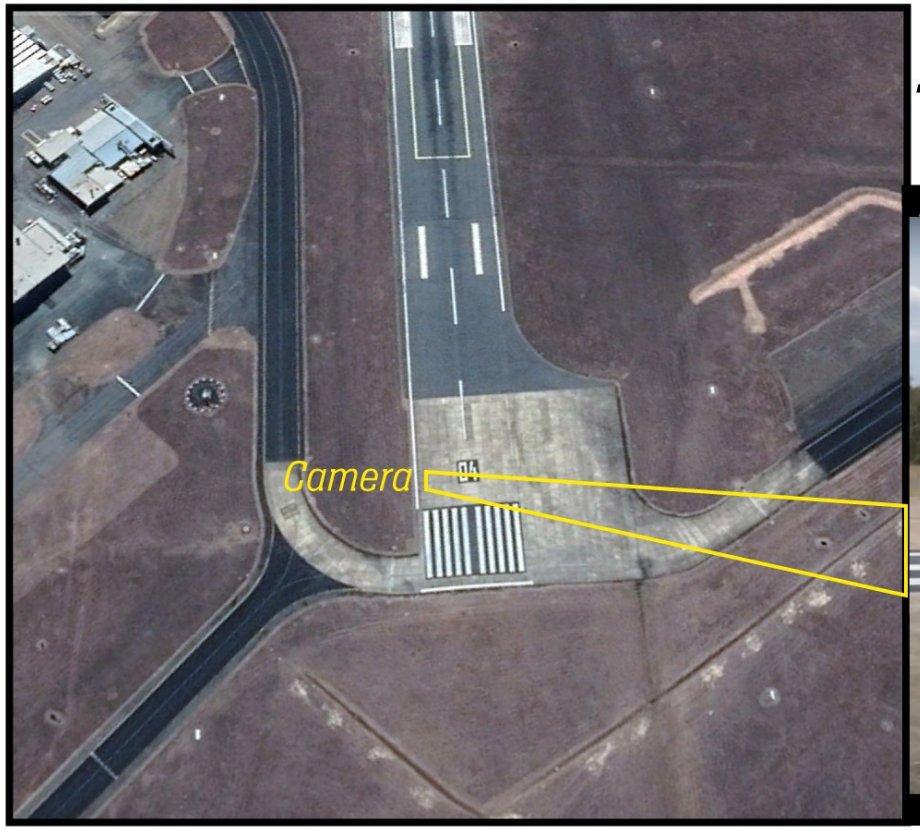
Staff that reveal the air base



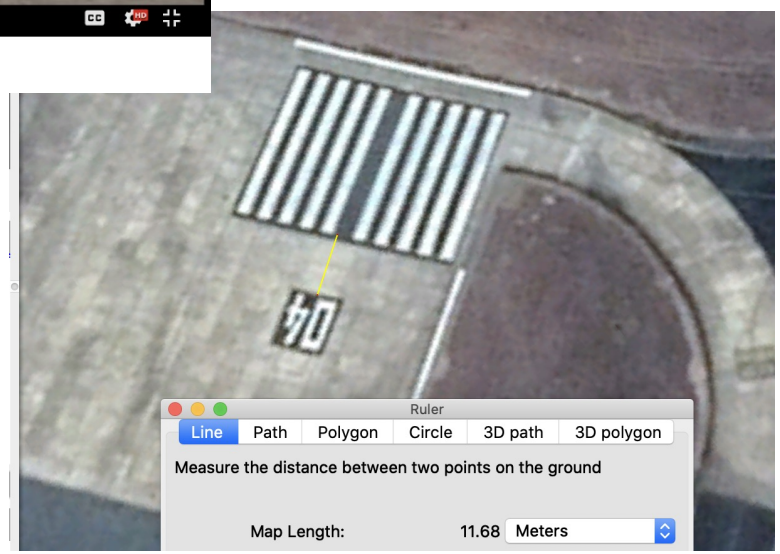
Checking social media posts

Amberley Airbase

Queensland, Australia



[Full investigation here]

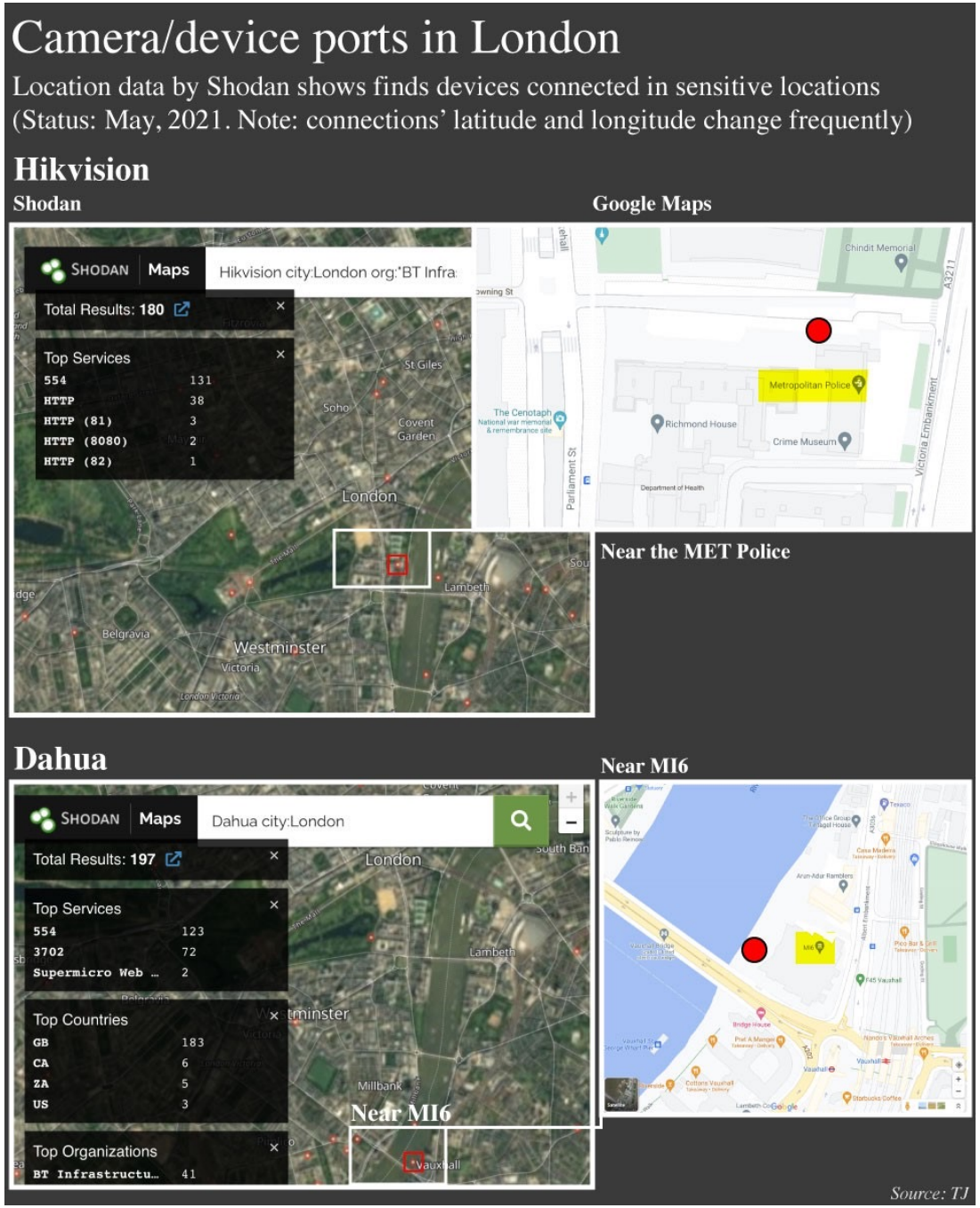


Spying with connected cams

Technical tools:

- Shodan (use search operators or map)
- Google Earth, Google StreetView

Full investigation



“Advanced Guide on Verifying Video Content” by Aric Toler

Verification & Analysis resources:
Advanced Guide on Verifying Video Content
face_recognition
How to verify photos and videos on social media networks
InVID Verification Plugin
Photo Verification Cheatsheet & Video Verification Cheatsheet
Verification 101
Verification Handbook

Aric Toler

Aric Toler started volunteering for Bellingcat in 2014 and has been on staff since 2015. He currently heads up Bellingcat's training and research efforts, with a focus on Eurasia/Eastern Europe.

Advanced Guide on Verifying Video Content

June 30, 2017 Fake News Geolocation

Translations: Русский

One of the most common issues for researchers and journalists is verifying user-generated video content, most often found on social networks and file sharing platforms, such as YouTube, Twitter, Facebook, and so on. There is no silver bullet to verify every video, and it may be nearly impossible to verify some videos short of acquiring the original file from the source. However, there is a range of methods we can use to verify most content, especially as it relates to making sure that videos showing breaking news events are not recycled from previous incidents. There are already numerous guides online for verifying video, most notably in the Verification Handbook. This guide will include some extra quirks frequently used by the Bellingcat team, and make an effort to provide our readers with ways to work around the limitations of the available tools. After reading this guide, hopefully you will not only know how to use this tool set, but also how to use creativity in avoiding dead ends.

ID/Personal verification:

Technical option:

- Reverse facial image search (TinEye, pimeyes.com)
- Facial images comparison (*face-api.js*; *MicrosoftAzure etc.*)
- Search operators (name)/social media analysis (what does the person post, how can we link it to other intelligence)

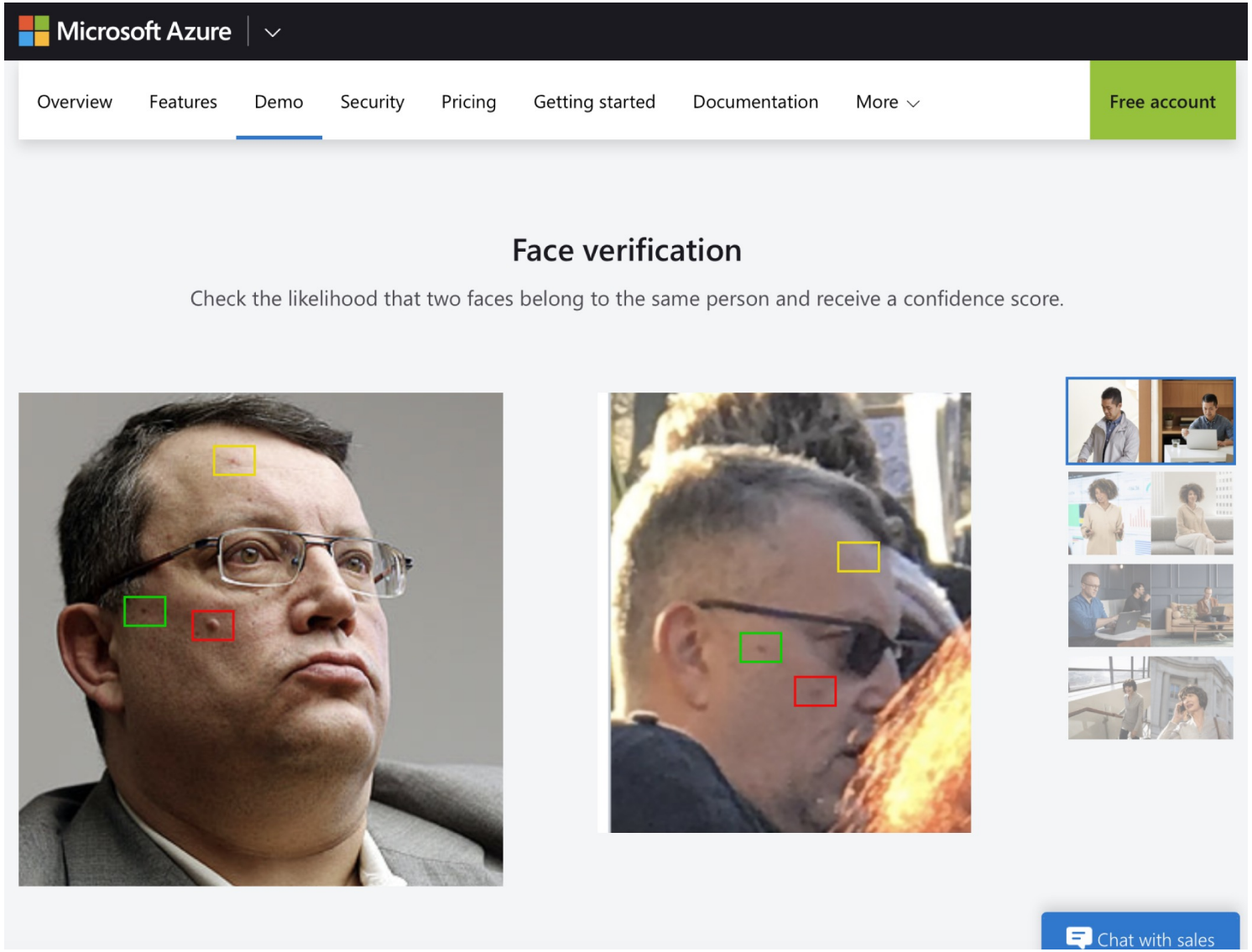
OSINT to track right-wing actors in Europe:

Topics:

- Telegram
- Interlinkages between actors' social media platforms
- Funding: Crypto traffic, donor models ('follow the bitcoin trail')

Visual verification: People

Case-study:



OSINT search on new social platforms

Telegram analysis

Trends

- Move to TG among right wing groups/individuals
- Away from Twitter/Instagram/Facebook
- Parler closed

Read full guide

Telegram analysis

Technical search options

- Google search (advanced search and operators)
- Search (Telegram desktop app)
- Download data from Telegram channel (Json)

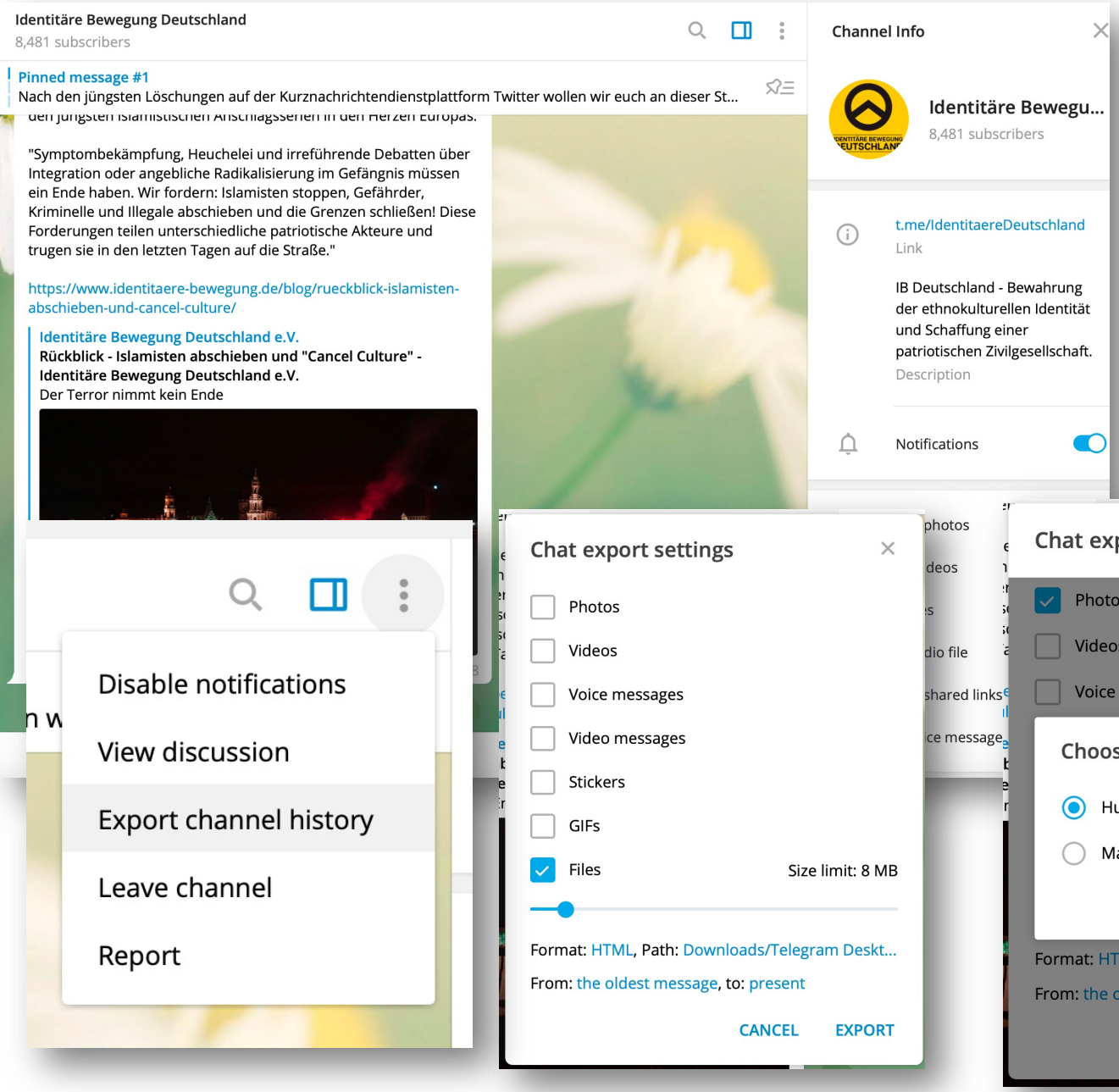
Read full guide

Telegram analysis – Guide

Technical analysis/tools

- Telegago
- tlgrm.eu (TG desktop app)
- tgstat.ru (Stats on TOMMY ROBINSON, a British far-right Islamophobic extremist acc. to HopeNotHate)
- Buzz.im (open message and channel search)
- Telegramchannels.me (preview channels without account)
- Run script that reformats data
- Telegram's API/Archive
- Easiest option: Json data channel history download re-formated by hand

Download TG data



Telegram analysis: data and network analysis

Case study: Generation Identity

- Download data from Telegram channel (Json)
- Turn into dataframe and search/analyze
- Turn into graph-data (network analysis)

Lambda, the symbol of the Identitarian movement/Identitarianism used primarily in Europe by Generation Identity and occasionally other countries, intended to commemorate the Battle of Thermopylae.

Telegram analysis: Network

Turn CSV into network diagram

Table 2 Net

Gephi

	Chat name	message ID	Name	ID	Message text	Message date an
0	IdentitaereDeutscl	1267	Identitäre Bewegung Deutschland		**EINE FAIRE DOKU?**🟥 Nicht wirklich aber "Vergiftete Heimat", die neueste Doku über sie IBD ist nicht uninteressant	2021/4/17, 12:9
1	IdentitaereDeutscl	1266	Identitäre Bewegung Deutschland		**Zu Gast: AfD-Troll Roger Beckamp!**Ihr kennt ihn sicherlich von seinen lustigen Antifa-Demo-Besuchen, bei denen de	2021/4/17, 7:12
2	IdentitaereDeutscl	1265	Identitäre Bewegung Deutschland			2021/4/4, 14:5
3	IdentitaereDeutscl	1264	Identitäre Bewegung Deutschland		Auch einige Patrioten waren in Stuttgart vor Ort und haben den großen Protest unterstützt 💪	2021/4/4, 14:5
4	IdentitaereDeutscl	1263	Identitäre Bewegung Deutschland		**AKTIONSVIDEO** - GEGEN DEN WIENER SCHANDSTEIN 🎓 Folgendes Aktionsvideo erreichte uns.🏷️ Mittlerweile be	2021/4/1, 11:40
5	IdentitaereDeutscl	1262	Identitäre Bewegung Deutschland			2021/4/1, 6:20
6	IdentitaereDeutscl	1261	Identitäre Bewegung Deutschland		**UNSER LEBEN WAR MEHR WERT ALS DAS**📰 Uns erreichte ein Bericht aus Wien:🗣️ "Um 06:00 fand in Wien am D	2021/4/1, 6:20
7	IdentitaereDeutscl	1260	Identitäre Bewegung Deutschland			2021/4/1, 5:34
8	IdentitaereDeutscl	1259	Identitäre Bewegung Deutschland			2021/4/1, 5:34
9	IdentitaereDeutscl	1258	Identitäre Bewegung Deutschland		Den heutigen Nachmittag nutzten unsere Aktivisten, um bei herrlichem Frühlingswetter mehrere hundert Flugblätter im H	2021/4/1, 5:34
10	IdentitaereDeutscl	1257	Identitäre Bewegung Deutschland		[](https://telegra.ph/file/0dd7cfa1fee26e86559a3.jpg)**Unser Computerspiel auf dem Index: Wir klagen!**Im Sommer let	2021/3/31, 13:34
11	IdentitaereDeutscl	1256	Identitäre Bewegung Deutschland		Absoluter Pflichttermin! Haltet euch heute Abend, 19 Uhr, frei. „Laut Gedacht" geht live - seid mit dabei!	2021/3/29, 10:22
12	IdentitaereDeutscl	1255	Identitäre Bewegung Deutschland		+++ Deutschland im Vormärz +++ Wie vor 200 Jahren nimmt die Zensur in Deutschland von Woche zu Woche zu. Nach	2021/3/27, 11:2
13	IdentitaereDeutscl	1254	Identitäre Bewegung Deutschland		Nach NGOs sind nun auch Bundestagsfraktionen von willkürlichen Zensurmaßnahmen betroffen.	2021/3/27, 11:2
14	IdentitaereDeutscl	1253	Identitäre Bewegung Deutschland		**Jetzt bei uns online: Die neue Folge "Laut Gedacht""Die erste Folge "Laut Gedacht", die nicht auf Youtube zu seher	2021/3/26, 21:49
15	IdentitaereDeutscl	1252	Identitäre Bewegung Deutschland		[](https://telegra.ph/file/dadaadb3413a4a21c91b9.jpg)**ZENSUR! UND JETZT?**Heute hat es "Laut Gedacht" getroffer	2021/3/26, 21:48
16	IdentitaereDeutscl	1251	Identitäre Bewegung Deutschland		**BEGEH GEDANKENVERBRECHEN! Protest gegen das ZDF in Hannover, WHO in Bonn und Pfizer in Berlin**Mit ihrer	2021/3/26, 18:6
17	IdentitaereDeutscl	1250	Identitäre Bewegung Deutschland			2021/3/19, 7:46
18	IdentitaereDeutscl	1249	Identitäre Bewegung Deutschland		Wofür in Deutschland der Verfassungsschutz zum Einsatz kommt, wird in Dänem	
19	IdentitaereDeutscl	1248	Identitäre Bewegung Deutschland		[](https://telegra.ph/file/c6e0189c510c9e51ac887.jpg)**Ja, ein Computerspiel wu	
20	IdentitaereDeutscl	1247	Identitäre Bewegung Deutschland		**Zensur, die es nicht gibt?**Wie berichtet man über etwas, was es gar nicht gibt	
21	IdentitaereDeutscl	1246	Identitäre Bewegung Deutschland		**Zeig Globalisten die rote Karte!**Mit Flugzetteln an Haustüren und mit einem B	
22	IdentitaereDeutscl	1245	Identitäre Bewegung Deutschland			
23	IdentitaereDeutscl	1244	Identitäre Bewegung Deutschland			
24	IdentitaereDeutscl	1243	Identitäre Bewegung Deutschland		Identitäre Aktivisten aus ganz Sachsen beteiligten sich heute in Dresden an den	
25	IdentitaereDeutscl	1242	Identitäre Bewegung Deutschland		Wer jetzt überlegt, ob er diese Meldung tatsächlich teilen kann, teilen darf, weil d	

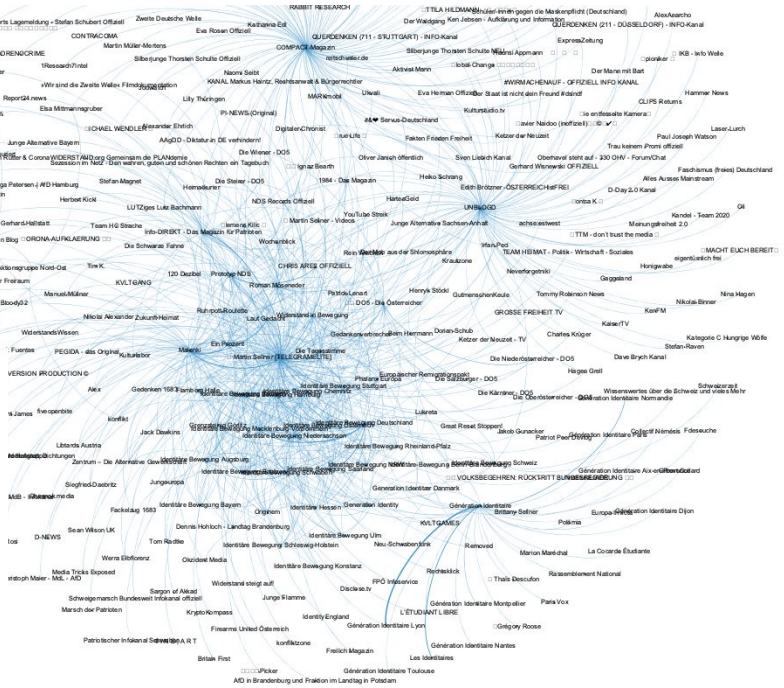
Table 2 Net

Load your CSV table

It has to be **comma-separated** and the first row must be dedicated to **column names**.

Choose file No file chosen

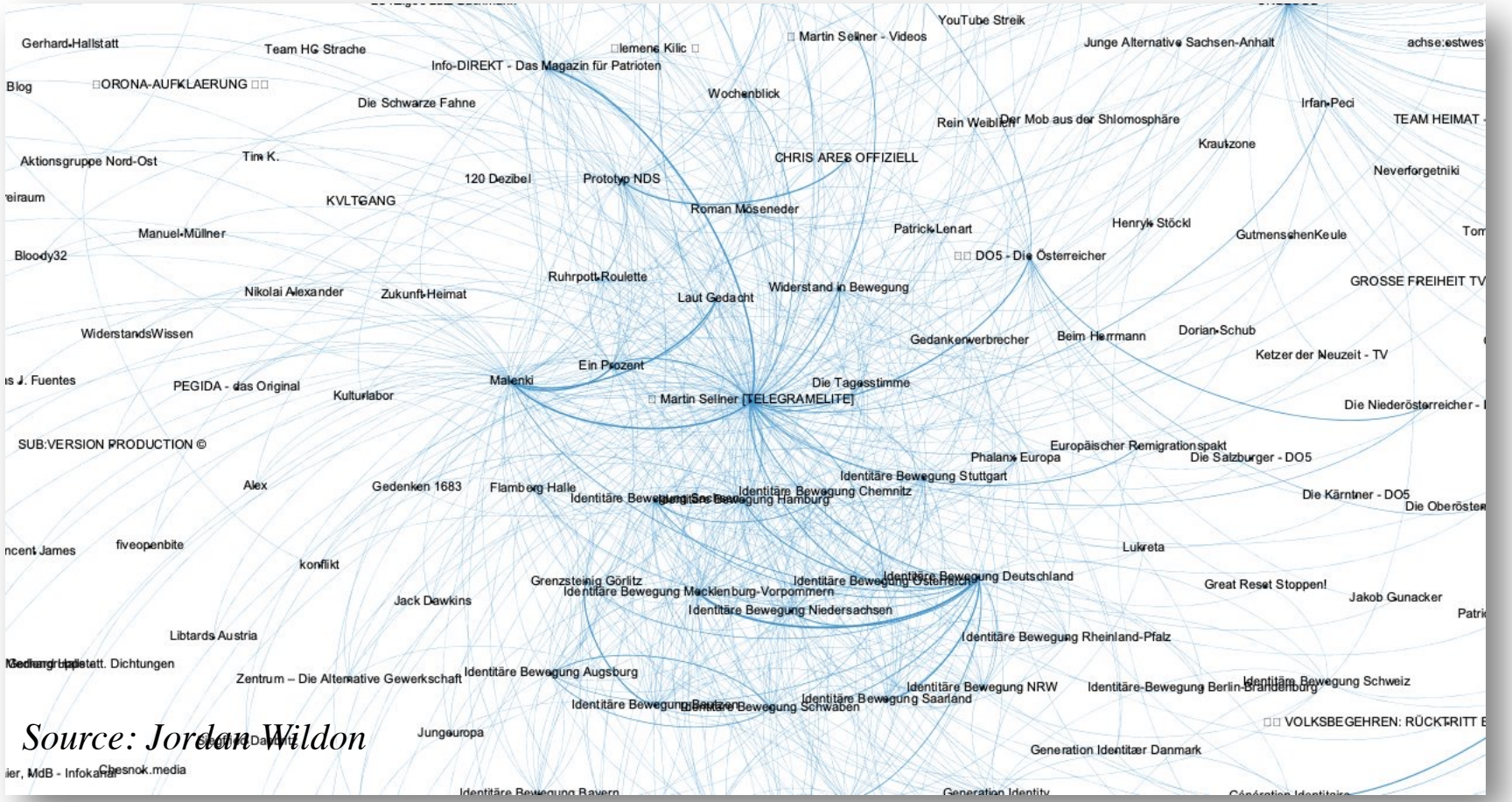
Note: you can drag and drop a file



Source: Jordan Wildon

Telegram analysis: Network

Identitäre Bewegung (IG) Deutschland (channel)



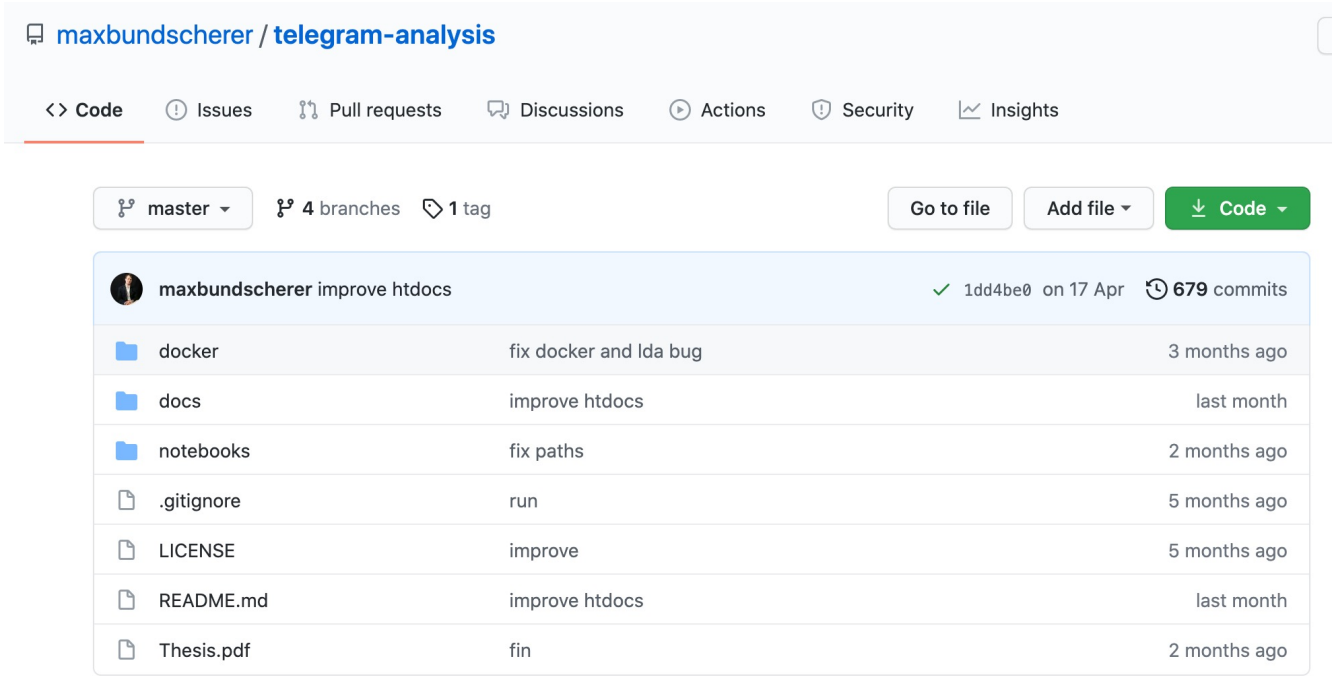
Source: Jordan Wildon

Findings: only a few account are instrumental in sharing posts

Gephi tutorial here

Telegram analysis: data and network analysis

Option: follow methodology for a telegram data science/mining project by [Maximilian Bundscherer]



Source: Jordan Wildon

OSINT to track virtual money streams:

Case study: GI & Martin Sellner (BBC)

- Generation Identify, a larger EU-wide Neo-Nazis movement
- Large groups developed in France, Germany and Austria
- Increasingly, appealing to the young
- Offer donors crypto donations (BIC)

Brittany Sellner 
@BrittPettibone

List of all the banks/platforms Martin has been banned from.

Folgende Plattformen und Zahlungsdienstleister haben mich bereits dauerhaft gesperrt:

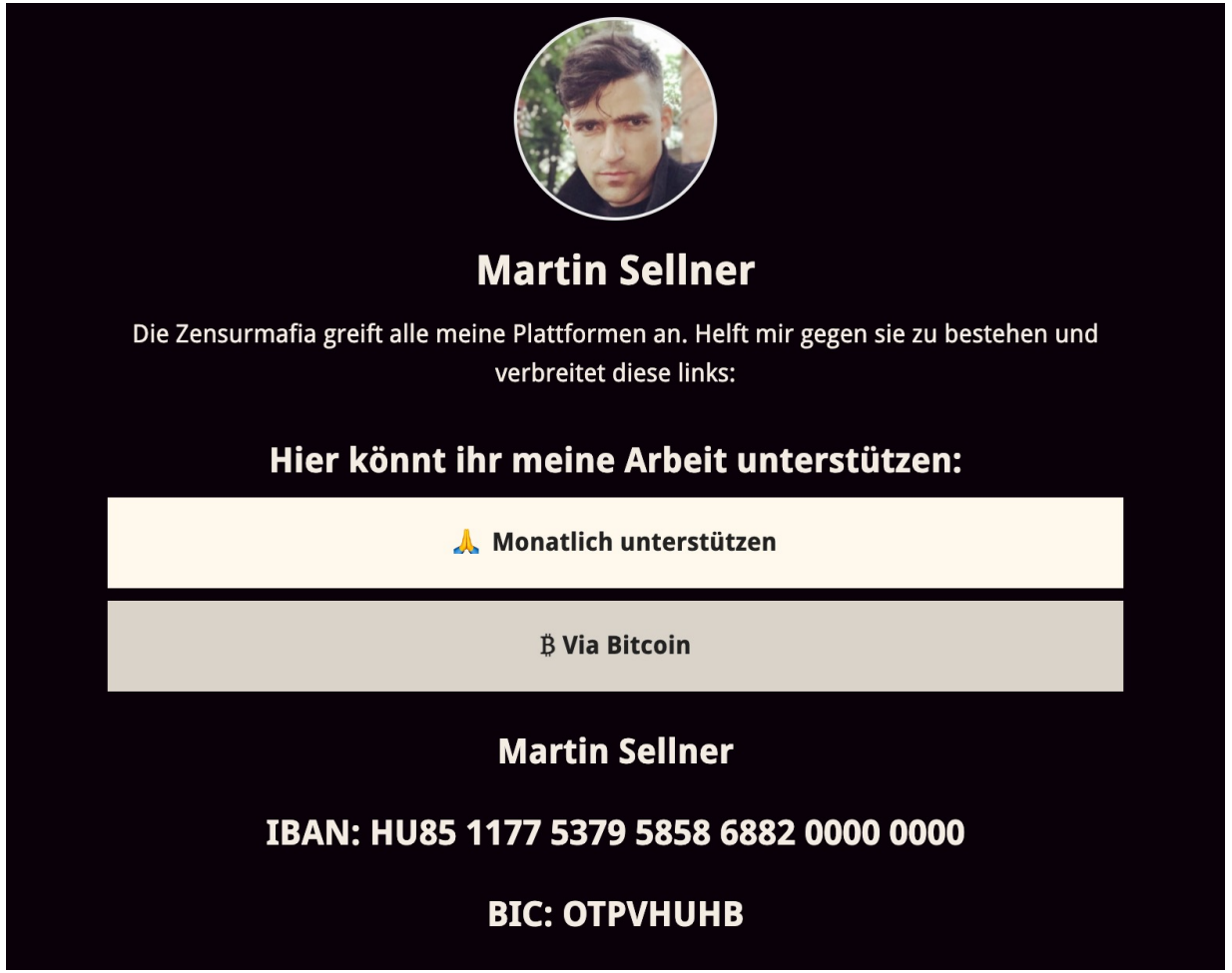
~~PayPal~~,
~~Patreon~~,
~~Facebook~~,
~~Instagram~~,
~~Gofundme~~,
~~Kickstarter~~,
~~STRIPE~~,
~~Bitpanda~~,
~~Twispay~~,
~~Go Cardless~~,
~~Maxpay~~,
~~Mollie~~,
~~Mailchimp~~,
~~Sendinblue~~

Folgende Banken haben mir das Konto gekündigt:

~~Raiffeisen Bank~~,
~~Bank Austria~~,
~~Monese Bank~~,
~~Ferratum Bank~~,
~~Austrian Anadi Bank~~,
~~N26 Bank~~,
~~RevolutBank~~,
~~Holvi Bank~~,
~~Fidor Bank~~,
~~Kontist Bank~~,
~~Deniz Bank~~,
~~Hello Bank~~,
~~Tatra Bank~~,
~~Oberbank~~,
~~BUNQ~~,
~~Tomorrow Bank~~,
~~Dadat Bank~~

OSINT and Bitcoin transactions: GI

- Search for old BC: Bitpanda (archived)
- Searching Bitcoin wallets: WhosWho
- New Bank accnt: Hungarian bank (Calcualator.com)
- $102,872 in BCCoin
- Bitcoinabuse analysis

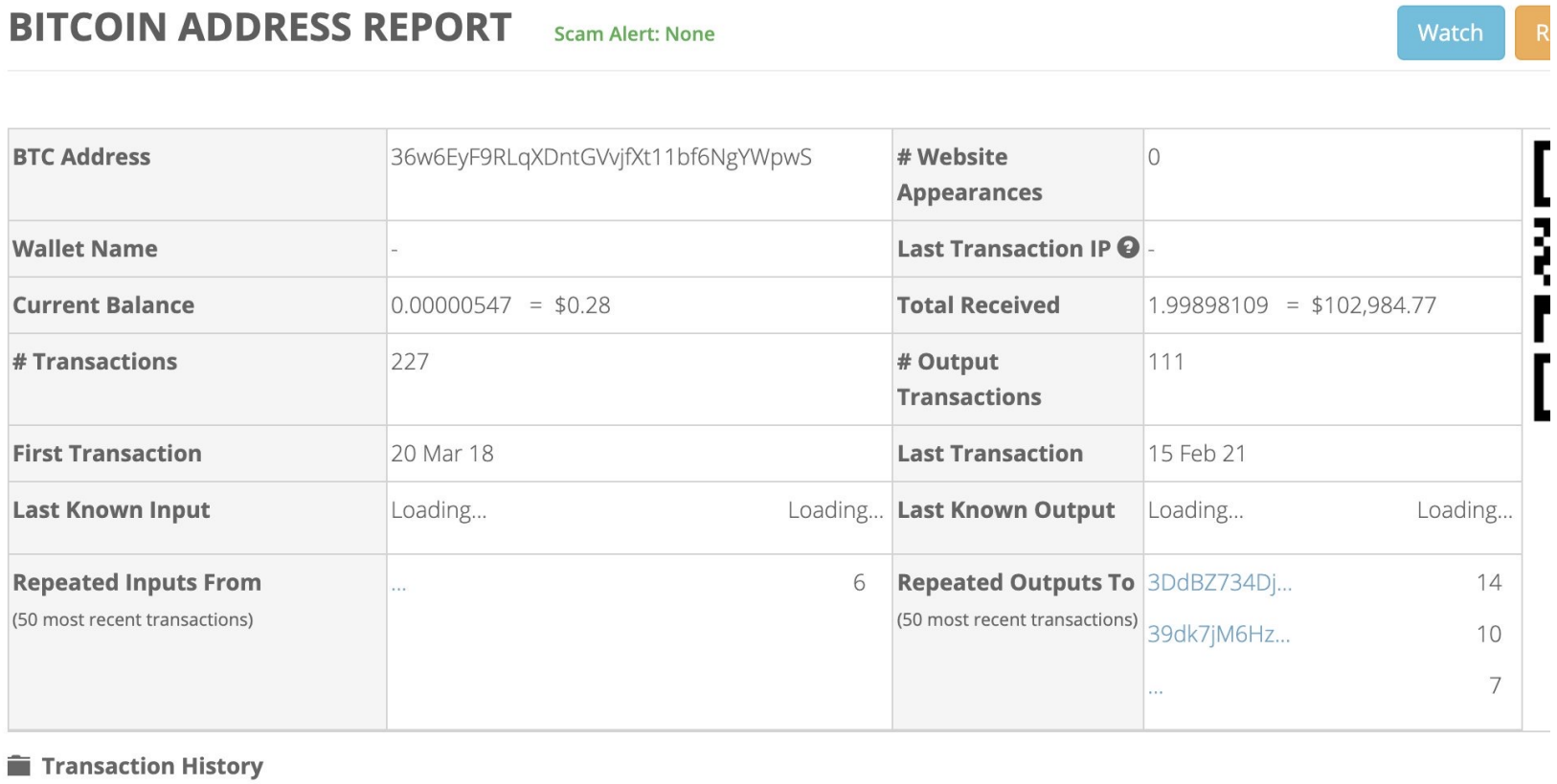


Bitcoin transaction records

[Read thread here]

e63aa6864b122912c45bde0642b7a3036181e2ac2c79870d9f98fc99dbb423ef				2020-07-06 03:07:22
36w6EyF9RLqXDntGVvjfXt11bf6NgYWpwS	→	3DdBZ734DjaqBf29PvjxWv9mvU6VaQEs8H 3E7vHYrWJaCi7hzhDSs1Ti6hC9UDaeC4hZ 3M49byha3x8fJVzV3TCpK3HmDm6Zgeb6G2 3LfUC7ZoqD1VTLXcWQAghsk1U6eKACutF5 1KYEwodFHZV1MeSSq3xFdGDfJBuB3J9qSj 3D8ZQHNfNrxr9SjzAMN73wTnYfEHiBdqC3 3MtZnNbTrwLdtx5Fu4fhjirDW5LPnFR283 3CtuECxYqTg52dv1viVkEsdAab3qb8YSCW	[http://Cryptoexploit]	0.17544617 BTC 20.00000000 BTC 0.05579298 BTC 0.00517772 BTC 0.36605712 BTC 0.00253743 BTC 0.00584241 BTC 0.00594000 BTC 0.00602993 BTC
0a910064945a909283dbbbda3a947ada6d92f139cbf39f12b714c68207ec605c				2020-07-06 02:38:27
1Mowps6xmhAHYQqohT6Z7vX6wXVCiXMFFu 1EPSsno265RTtgcKfqUeZMU7RxE1NPZtSK	→	36w6EyF9RLqXDntGVvjfXt11bf6NgYWpwS		0.00121100 BTC
cc7bc4e4b0d39c2aa78c41763e8a24d44a400c196ccfb42a535f17b742c7818e				2020-06-04 01:14:14
36w6EyF9RLqXDntGVvjfXt11bf6NgYWpwS	→	3DdBZ734DjaqBf29PvjxWv9mvU6VaQEs8H 1CqNbJbFiR46KnhfvjM4EQ1vDQeCqL7rXh 33hqbweb4riN6ATiggLYBQYn8NQehjhHEa 3Bxp3qd89dPtSb5MUieSX9Zy3HT3PJFv2s	[http://Cryptoexploit]	8.75361789 BTC 0.01862003 BTC 0.00190051 BTC 0.02800000 BTC 0.29977460 BTC
4e7e6680bcc08d8c8fa6fea407afa9d6b0a69204d662e3f1e6a61f858982edec				2020-06-03 23:39:54
1JGzmcmYULBG8Sj6TtwY14bc4hHZPpDE7V	→	36w6EyF9RLqXDntGVvjfXt11bf6NgYWpwS		0.00125000 BTC
c27aa4908cfffd5bf87f7adfc14e5a7f17c671023df834026c055bf8db802350				2020-05-02 07:31:02
36w6EyF9RLqXDntGVvjfXt11bf6NgYWpwS	→	3DdBZ734DjaqBf29PvjxWv9mvU6VaQEs8H 34pxoykTJt3pLHRiXmtERMRAmbKyaCyD7w 38ZzBZMdjHRWFUvA5yYZ78Z4ZSfY8yXrZB 3No75NkXoYb58FJrWGGb6J8rRARZDEgzH3 3Mo5e5YhXasPEmB6FQvmmfnsErePNLa6mT 1FJ3CPrhEjGDbTevj5kGf1BmmogewWGorC	[http://Cryptoexploit]	9.72480764 BTC 0.04258734 BTC 0.00493449 BTC 0.00254784 BTC 0.03925856 BTC 0.00537163 BTC
1feb28866ce8fafd8e8fe94da044799a560c55051abdecde88c5e5b3e6daccea				2020-05-02 07:23:11
1KzPPBRpBWWAAcRyNPBMc2BxbdzwBS4gL	→	36w6EyF9RLqXDntGVvjfXt11bf6NgYWpwS		0.00125000 BTC
6977361906d10d9df159e1461ce326760cc59e6be83785aeb2719a6f0e7775ae				2020-04-05 12:00:59
36w6EyF9RLqXDntGVvjfXt11bf6NgYWpwS	→	3DdBZ734DjaqBf29PvjxWv9mvU6VaQEs8H 35u8MEzoBqVFYr3rjFL3z8XJTYPfJdG6yt 1Gq2ip3E5Nxb4LFSAA9C4GMJg9pa96QjZp 36U7NTNNrGWg6iMmStcMv9ueRhWrhs7QSi	[http://Cryptoexploit]	5.27078835 BTC 0.00552212 BTC 0.02300000 BTC 0.01484607 BTC

OSINT and Bitcoin transactions: GI



BITCOIN ADDRESS REPORT

Scam Alert: None

Watch R

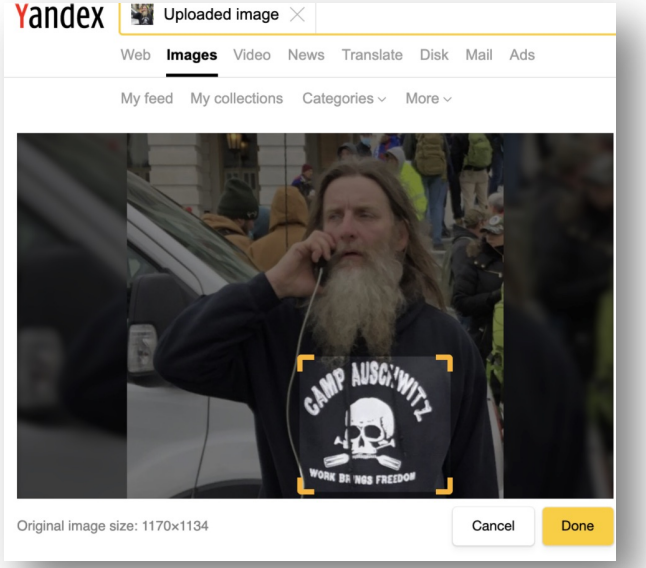
BTC Address	36w6EyF9RLqXDntGVvjfXt11bf6NgYWpwS	**# Website Appearances**	0
Wallet Name	-	**Last Transaction IP**	-
Current Balance	0.00000547 = $0.28	**Total Received**	1.99898109 = $102,984.77
# Transactions	227	**# Output Transactions**	111
First Transaction	20 Mar 18	**Last Transaction**	15 Feb 21
Last Known Input	Loading... Loading...	**Last Known Output**	Loading... Loading...
Repeated Inputs From (50 most recent transactions)	... 6	**Repeated Outputs To** (50 most recent transactions)	3DdBZ734Dj... 14 39dk7jM6Hz... 10 ... 7

Transaction History

Tracking right wing visual markers with OSINT

OSINT to analyse

- *Merchandise*
- *Clothing*
- *Hand signals*
- *Symbolism*
- *Fonts*
- *Signs*



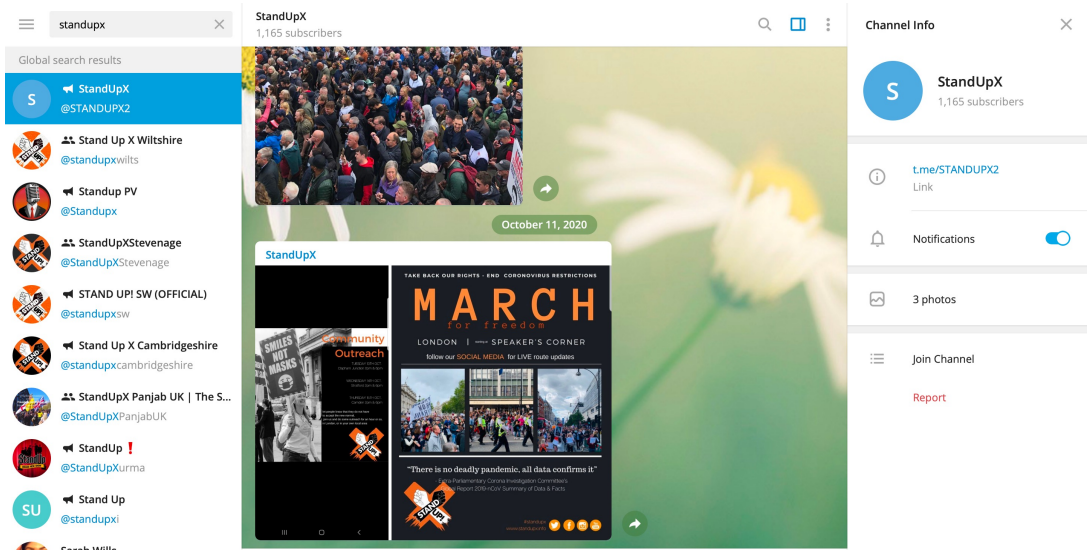
Credit: Jim Urquhart/Reuters; Sidenote: here an interesting Twitter thread by Scott Railton on the person with the orange hat in the building

[Read training post here]

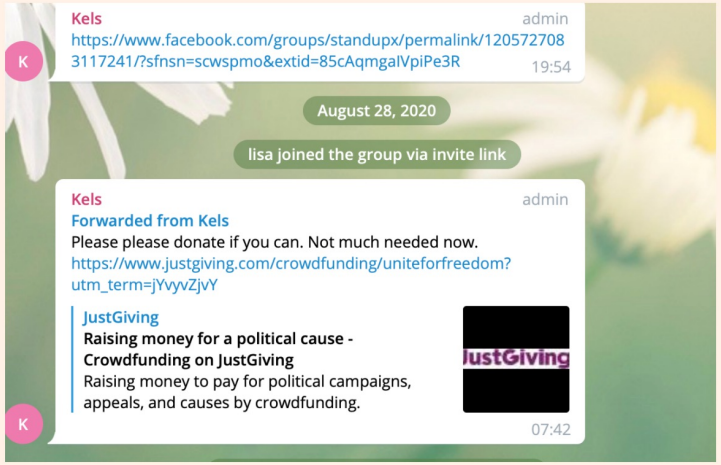
OSINT and social media identities: StandUpX

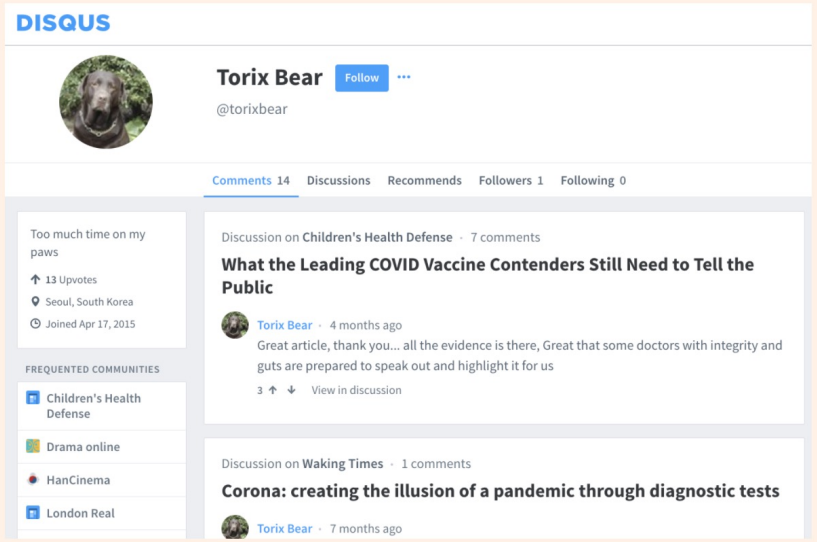
- Username analysis allows us to gather intelligence on how individuals jump from platform to platform. Research on UK Telegram group, a StandupX, a larger anti-lockdown movement that was banned from the conventional platform of Twitter and Facebook, moved to new, alternative platforms. OSINT allowed to understand who administrators are who how they orchestrate the groups in the background

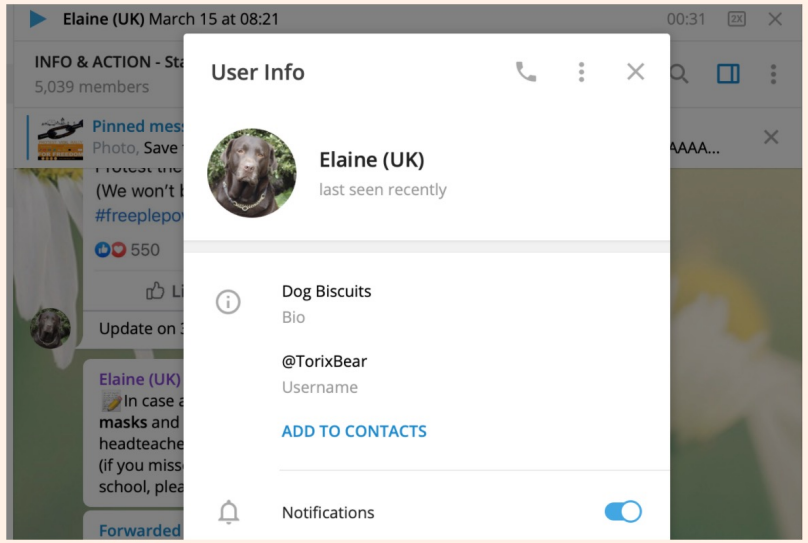
Read investigation here



OSINT and social media identities: StandUpX





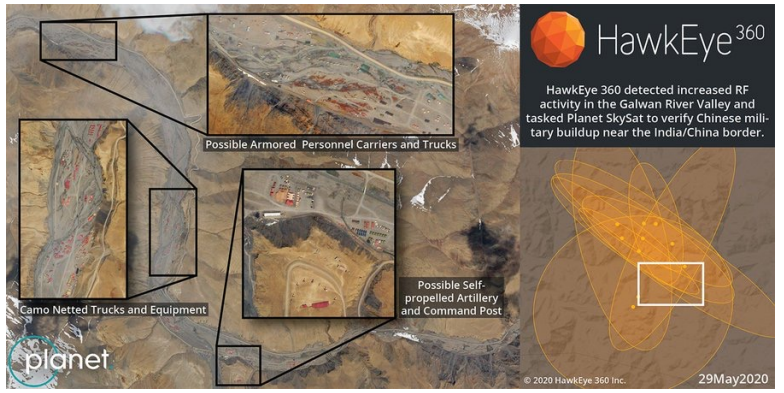


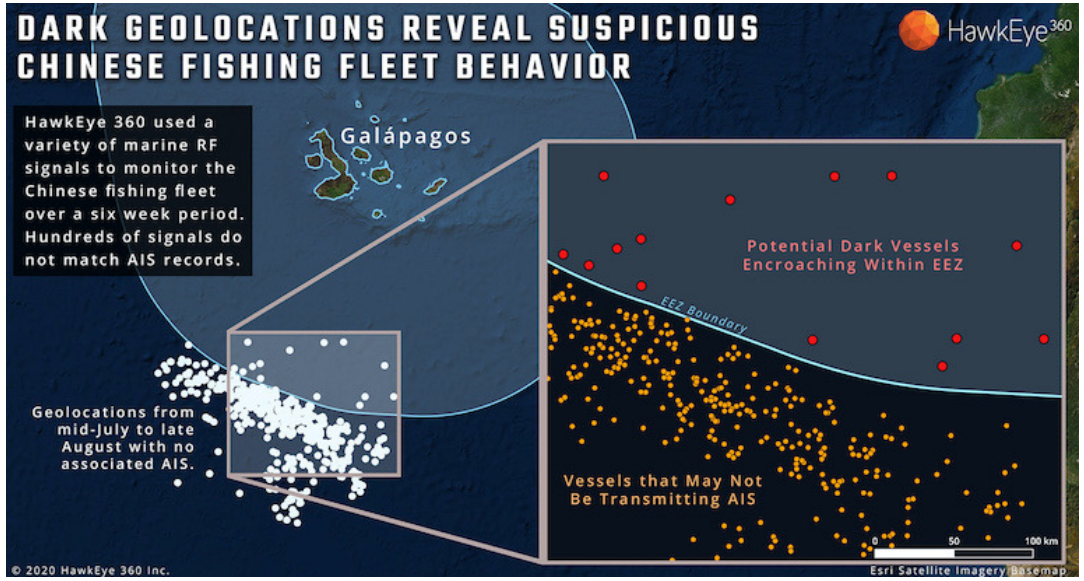
The 'Elaine (UK)' aka ToxicBear handle is found on other platforms

[Read investigation here]

New satellite source: RF

- RF signals emitted by ships through their navigation radars and radio communications



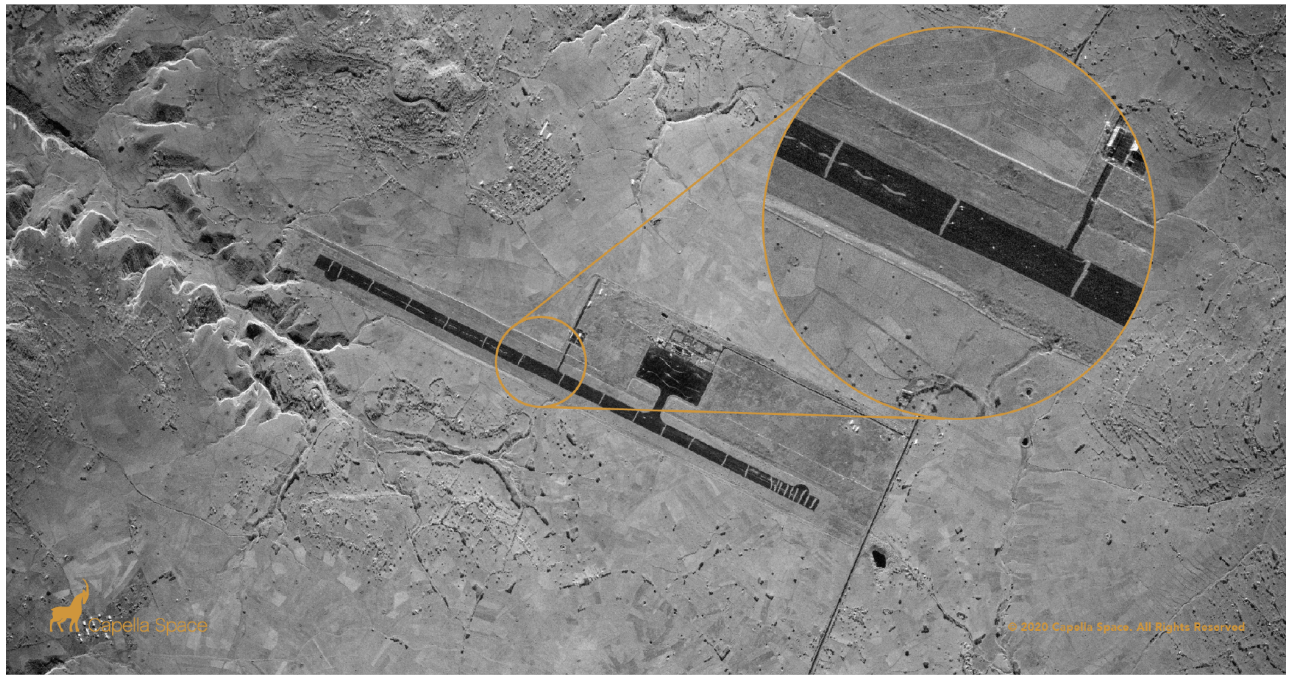


[Read training posts here]

New Satellite source: SAR

- Synthetic Aperture Radar (SAR) imagery. SAR data is microwave data sent by an active sensor.

[Read training posts here]



SAR image example: Image of Aksum Airport (in the northern Tigray Region of Ethiopia), captured during the Tigray conflict when the Tigray People's Liberation Front sabotaged the runway before falling to federal forces. Smooth tarmac absorbs radar energy and dirt from the trenches dug across the runway are much brighter in comparison (Capella).

Illegal wildlife trade: what is it?

- Elephant ivory, illegal trophies, live-animals
- Traded on online auction sites (eBay, Facebook)

[Read thread here]

Useful links

- Brazell (Book)
- Bellingcat:
- https://docs.google.com/spreadsheets/d/18rtqh8EG2q1xBo2cLNyhIDuK9jrPGwYr9DI2UncoqJQ/edit#gid=1130825724
- Ben Strick
- https://benjaminstrick.com/geospatial-awareness-how-to-add-data-to-google-earth/
- Resources - DDJ
- https://github.com/r3mlab/datajournalism-resources
- OSINT resources:
- https://intelligence.is/open-source-intelligence-osint-tools/

Thanks

Connect on Twitter
via @BenHeubl