

Advanced OSINT & Introduction to Maltego

Using Github Tools & Basic Maltego Investigations

Google Cloud Shell

The Cloud Shell interface is split into three sections:

- Blue: File system explorer
- Red: File preview
- Green: Console interface

The screenshot shows the Google Cloud Shell interface divided into three main sections:

- Explorer (Blue Section):** Shows the file system structure under "SSIIIXX". It includes a folder named "sherlock" and a file named "file.csv". The "file.csv" file is currently selected.
- Preview (Red Section):** Displays the contents of the "file.csv" file. The data consists of 11 rows of comma-separated values (CSV). The columns include: id, conversation_id, created_at, date, time, timezone, user_id, username, name, place, tweet, and language. All entries have an "id" starting from 1 and a "language" value of "+0000".
- Terminal (Green Section):** Shows a command-line session. The user runs `pip install requests` and `pip install requests-futures stem torrequest`. They then run `python3 sherlock nordfront` which performs a search. The results show several websites such as Academia.edu, AskFM, Bandcamp, Blogger, CNET, and Championat, all associated with the "nordfront" keyword.

```
Requirement already satisfied: idna<3,>=2.5 in /usr/local/lib/python3.7/dist-packages (from requests>=2.22.0->-r requirements.txt (line 7)) (2.10)
Requirement already satisfied: urllib3!=1.25.0,!=1.25.1,<1.26,>=1.21.1 in /usr/local/lib/python3.7/dist-packages (from requests>=2.22.0->-r requirements.txt (line 7)) (1.25.11)
Requirement already satisfied: chardet<4,>=3.0.2 in /usr/local/lib/python3.7/dist-packages (from requests>=2.22.0->-r requirements.txt (line 7)) (3.0.4)
Building wheels for collected packages: bs4, requests-futures, stem, torrequest
  Running setup.py bdist_wheel for bs4 ... done
  Stored in directory: /home/ssiiixx/.cache/pip/wheels/a0/b0/b2/4f80b9456b87abedbc0bf2d52235414c3467d8889be38dd472
  Running setup.py bdist_wheel for requests-futures ... done
  Stored in directory: /home/ssiiixx/.cache/pip/wheels/26/d0/f5/dc4e4a37bbe55c9acf967d2bd899152412c1e49c227f5395ff
  Running setup.py bdist_wheel for stem ... done
  Stored in directory: /home/ssiiixx/.cache/pip/wheels/02/3a/ee/1094b166e029353f892c0b121aa02f48aff5e658396924bc2a
  Running setup.py bdist_wheel for torrequest ... done
  Stored in directory: /home/ssiiixx/.cache/pip/wheels/db/dd/d0/b7a91fb9e5a22df60bd93460ed2d0e75c3932f00e3f464a8fc
Successfully built bs4 requests-futures stem torrequest
Installing collected packages: bs4, requests-futures, stem, torrequest
Successfully installed bs4-0.0.1 requests-futures-1.0.0 stem-1.8.0 torrequest-0.1.0
ssiiixx@cloudshell:~/sherlock$ python3 sherlock nordfront
[*] Checking username nordfront on:
[+] Academia.edu: https://independent.academia.edu/nordfront
[+] AskFM: https://ask.fm/nordfront
[+] Bandcamp: https://www.bandcamp.com/nordfront
[+] Blogger: https://nordfront.blogspot.com
[+] CNET: https://www.cnet.com/profiles/nordfront/
[+] Championat: https://www.championat.com/user/nordfront
```

Debian Linux Basics

For getting around:

ls - list the contents of the folder you are in

cd - change directory (move to another folder),

cd .. - will take you back up one directory

git clone - download a program from Github to your computer

python3 - programming language of the tools we're working with

Installing a Program

Installing programs will be done from Github, you can see instructions for our first program here:

<https://github.com/laramies/theHarvester/wiki/Installation>

Option 3 - From Source (No Pipenv)

The third option is building from source, simply run these commands and you are all set!
Make sure you are using Python3.7+

```
$ ~ > git clone https://github.com/laramies/theHarvester
$ ~ > cd theHarvester

If developing do:
    $ ~ > python3 -m pip install -r requirements/dev.txt
Else:
    $ ~ > python3 -m pip install -r requirements/base.txt

$ ~ > python3 theHarvester.py -h
```

First program: TheHarvester

This program discovers email addresses, and profiles a domain to find more information about it.

We can see the results on the screen, or save them as a file.

```
Searching 500 results.  
[*] Searching LinkedIn.  
  
[*] Links found: 5  
-----  
https://www.linkedin.com/in/aaliyah-nord-048b78122  
https://www.linkedin.com/in/dawn-nord-564945a5  
https://www.linkedin.com/in/edward-nord-a3b0881b9  
https://www.linkedin.com/in/nichole-nord-39532395  
https://www.linkedin.com/in/rebecca-nord-11202612b  
  
[*] IPs found: 14  
-----  
37.123.176.5  
37.123.176.28  
104.24.178.11  
104.24.179.11  
104.25.150.31  
104.25.151.31  
104.27.118.114  
104.27.119.114  
172.67.81.93  
2606:4700:30::681b:92cb  
2606:4700:30::681b:93cb  
  
[*] Emails found: 1  
-----  
redaktionen@nordfront.se  
  
[*] No hosts found.
```

GitHub Basics

To install a program from Github:

Installation

```
# clone the repo  
$ git clone https://github.com/sherlock-project/sherlock.git  
  
# change the working directory to sherlock  
$ cd sherlock  
  
# install the requirements  
$ python3 -m pip install -r requirements.txt
```

- Go to the Github page of the program you want to install
- Open a terminal on your computer (the cloud shell) and use the **git clone** command to download the program
- Use the `cd` command to move into the folder that holds the downloaded program
- Follow the installation instructions on the Github page

Installing Sherlock

Our first tool to use will be Sherlock, we'll install it with the following command:

```
git clone https://github.com/sherlock-project/sherlock.git && cd sherlock &&  
python3 -m pip install -r requirements.txt
```

Read the Help File

Look at available commands using the following command:

python3 sherlock --help

```
ssiiixx@cloudshell:~/sherlock$ python3 sherlock --help
usage: sherlock [-h] [--version] [--verbose] [--folderoutput FOLDEROUTPUT]
                 [--output OUTPUT] [--tor] [--unique-tor] [--csv]
                 [--site SITE_NAME] [--proxy PROXY_URL] [--json JSON_FILE]
                 [--timeout TIMEOUT] [--print-all] [--print-found] [--no-color]
                 [--browse] [--local]
                 USERNAMES [USERNAMES ...]
```

Sherlock: Find Usernames Across Social Networks (Version 0.13.0)

positional arguments:

```
    USERNAMES           One or more usernames to check with social networks.
```

optional arguments:

```
    -h, --help            show this help message and exit
    --version             Display version information and dependencies.
    --verbose, -v, -d, --debug
                          Display extra debugging information and metrics.
    --folderoutput FOLDEROUTPUT, -fo FOLDEROUTPUT
                          If using multiple usernames, the output of the results
                          will be saved to this folder.
    --output OUTPUT, -o OUTPUT
                          If using single username, the output of the result
                          will be saved to this file.
    --tor, -t              Make requests over Tor; increases runtime; requires
```

Screen Name Search

Run a search for a screen name with the following command:

python3 sherlock nordfront

Make sure to run **cd ..** before we install the next program!

```
ssiiixx@cloudshell:~/sherlock$ python3 sherlock nordfront
[*] Checking username nordfront on:
[+] Academia.edu: https://independent.academia.edu/nordfront
[+] AskFM: https://ask.fm/nordfront
[+] Bandcamp: https://www.bandcamp.com/nordfront
[+] Blogger: https://nordfront.blogspot.com
[+] CNET: https://www.cnet.com/profiles/nordfront/
[+] Championat: https://www.championat.com/user/nordfront
[+] Codecademy: https://www.codecademy.com/profiles/nordfront
[+] DailyMotion: https://www.dailymotion.com/nordfront
[+] DeviantART: https://nordfront.deviantart.com
[+] Discogs: https://www.discogs.com/user/nordfront
[+] Disqus: https://disqus.com/nordfront
[+] Duolingo: https://www.duolingo.com/profile/nordfront
[+] Ebay: https://www.ebay.com/usr/nordfront
[+] Euw: https://euw.op.gg/summoner/userName=nordfront
[+] F3.cool: https://f3.cool/nordfront/
[+] Facebook: https://www.facebook.com/nordfront
[+] FortniteTracker: https://fortnitetracker.com/profile/all/nordfront
[+] Giphy: https://giphy.com/nordfront
[+] GitHub: https://www.github.com/nordfront
[+] Gravatar: http://en.gravatar.com/nordfront
[+] Imgur: https://imgur.com/user/nordfront
[+] Instagram: https://www.instagram.com/nordfront
[+] Kik: https://kik.me/nordfront
[+] LiveJournal: https://nordfront.livejournal.com
[+] LiveLeak: https://www.liveleak.com/c/nordfront
[+] Medium: https://medium.com/@nordfront
[+] Myspace: https://myspace.com/nordfront
[+] NameMC (Minecraft.net skins): https://namemc.com/profile/nordfront
[+] Newgrounds: https://nordfront.newgrounds.com
[+] Periscope: https://www.periscope.tv/nordfront/
[+] Pinterest: https://www.pinterest.com/nordfront/
[+] PromoDJ: http://promodj.com/nordfront
[+] Quora: https://www.quora.com/profile/nordfront
[+] Rajce.net: https://nordfront.rajce.idnes.cz/
[+] Realmeye: https://www.realmeye.com/player/nordfront
[+] Reddit: https://www.reddit.com/user/nordfront
```

Installing TheHarvester

You can install TheHarvester by pasting the following commands into your terminal:

```
git clone https://github.com/laramies/theHarvester
```

```
cd theHarvester
```

```
python3 -m pip install -r requirements/base.txt
```

Or, you can do it all in one command:

```
git clone https://github.com/laramies/theHarvester && cd theHarvester &&  
python3 -m pip install -r requirements/base.txt
```

Read the Help Menu

To see the available options, run the following command:

python3 theHarvester.py -h

Simple Search

```
theHarvester.py -d www.nordfront.se -b all -f nordemail.html
```

theHarvester Scan Report					
Overall statistics					
Domains	Hosts	IP Addresses	Vhosts	Emails	Shodan
1	6	52	0	4	0

Latest scan report

Date	Domain	Plugin	Record	Result
2020-11-09	www.nordfront.se	bing	email	redaktionen@nordfront.se
2020-11-09	www.nordfront.se	bing	email	redaktionen@nordfront.se

Let's Use More Arguments

After looking at the help file, let's try using more of the arguments to give us more information:

```
python3 theHarvester.py -d www.nordfront.se -g -v -n -c -b all -f nord.html
```

```
-g, --google-dork      Use Google Dorks for Google search.  
-p, --proxies         Use proxies for requests, enter proxies in proxies.yaml.  
-s, --shodan          Use Shodan to query discovered hosts.  
--screenshot Screenshot      Take screenshots of resolved domains specify output directory: --screenshot output_directory  
-v, --virtual-host    Verify host name via DNS resolution and search for virtual hosts.  
-e DNS_SERVER, --dns-server DNS_SERVER      DNS server to use for lookup.  
-t DNS_TLD, --dns-tld DNS_TLD      Perform a DNS TLD expansion discovery, default False.  
-r, --take-over       Check for takeovers.  
-n, --dns-lookup      Enable DNS server lookup, default False.  
-c, --dns-brute       Perform a DNS brute force on the domain.
```

Previous scan report

Sample Report

You can download & open a sample report in your browser:

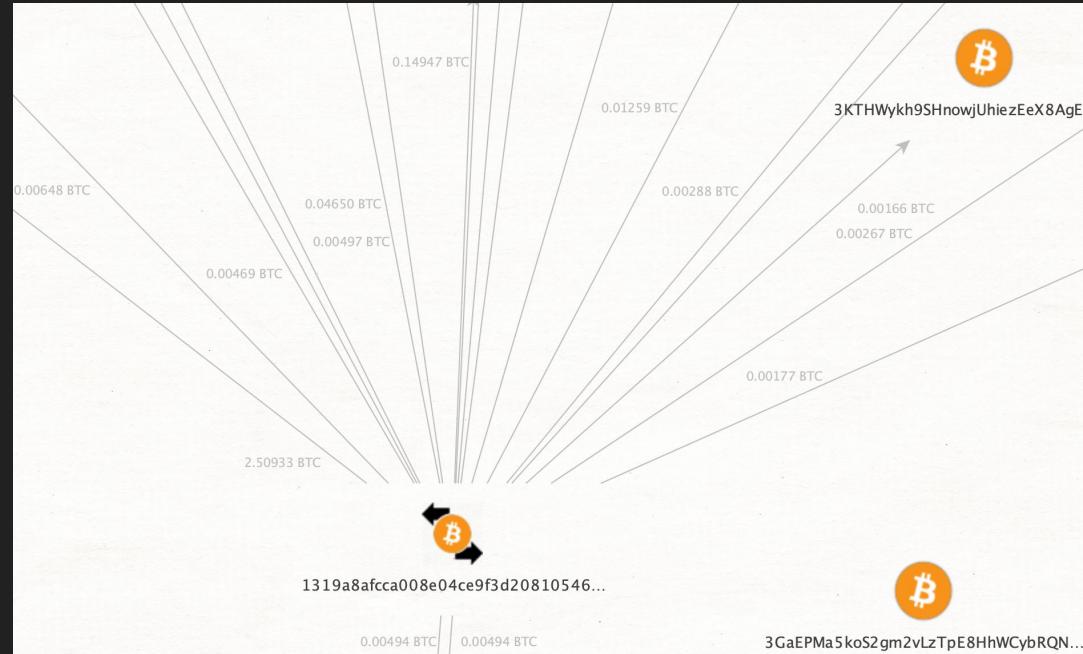
<https://raw.githubusercontent.com/ski ckar/OSINT2020/main/nord.html>

Date	Domain	Plugin	Record type	Result
2020-11-09	www.nordfront.se	bing	email	redaktionen@nordfront.se
2020-11-09	www.nordfront.se	bufferoverun	ip	104.25.150.31
2020-11-09	www.nordfront.se	bufferoverun	ip	104.27.119.114
2020-11-09	www.nordfront.se	bufferoverun	ip	2606:4700:30::681b:93cb
2020-11-09	www.nordfront.se	bufferoverun	ip	2606:4700:30::681b:92cb
2020-11-09	www.nordfront.se	bufferoverun	ip	104.25.151.31
2020-11-09	www.nordfront.se	bufferoverun	ip	172.67.81.93
2020-11-09	www.nordfront.se	bufferoverun	ip	104.24.178.11
2020-11-09	www.nordfront.se	bufferoverun	ip	104.24.179.11
2020-11-09	www.nordfront.se	dns_bruteforce	host	dev.nordfront.se:172.67.81.93, 104.24.179.11, 104.24.178.11
2020-11-09	www.nordfront.se	dns_bruteforce	host	forum.nordfront.se:172.67.81.93, 104.24.178.11, 104.24.179.11
2020-11-09	www.nordfront.se	dns_bruteforce	host	it.nordfront.se:172.67.81.93, 104.24.178.11, 104.24.179.11
2020-11-09	www.nordfront.se	dns_bruteforce	host	media.nordfront.se:172.67.81.93, 104.24.179.11, 104.24.178.11
2020-11-09	www.nordfront.se	dns_bruteforce	host	wiki.nordfront.se:104.24.178.11, 172.67.81.93, 104.24.179.11
2020-11-09	www.nordfront.se	dns_bruteforce	host	www.nordfront.se:172.67.81.93, 104.24.179.11, 104.24.178.11
2020-11-09	www.nordfront.se	google	name	https://www.linkedin.com/in/edward-nord-a3b0881b9
2020-11-09	www.nordfront.se	google	name	https://www.linkedin.com/in/rebecca-nord-11202612b
2020-11-09	www.nordfront.se	google	name	https://www.linkedin.com/in/aaliyah-nord-048b78122
2020-11-09	www.nordfront.se	google	name	https://www.linkedin.com/in/dawn-nord-564945a5
2020-11-09	www.nordfront.se	google	name	https://www.linkedin.com/in/nichole-nord-39532395

Maltego Basics

Maltego is an advanced OSINT tool designed to make a few parts of OSINT more easy:

- Visualizing data
- Using API's to pull in new data
- Organizing relationships between data points



Download Maltego

Navigate to the following URL to download Maltego for your operating system:

<https://www.maltego.com/downloads/>

DOWNLOADS

Select your operating system and filetype.

Windows

Linux

Mac



Maltego for Mac

SELECT A FILE TYPE

.dmg

DOWNLOAD MALTEGO

MD5 Hash

7e453730898c5e018376c142caffbaee

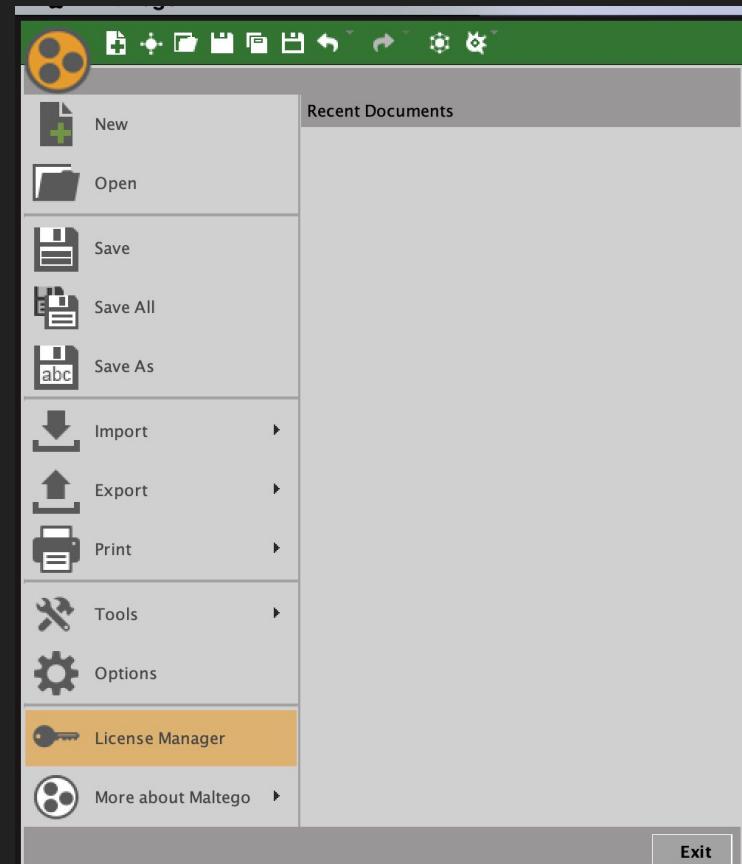
SHA256 Hash

d1db4084c4861c552575734689c10b53e2d669ad45fab78b9dc91a572766ae75

Install Your License Key

Included with this class, you should have received a Maltego Classic license key.

Input your key when Maltego asks for it during the installation, or you can always install the free community edition and add your license in the license manager later.



What Are Transforms?

Transforms fetch data and organize it visually, using data types called entities.

TRANSFORM HUB PARTNERS 11/58 shown



Standard Transforms

by Maltego Technologies

Free Standard OSINT Transforms

New



CaseFile Entities

by Paterva

Additional entities from CaseFile



ATT&CK – MISP

by MISP Project

Query data from MISP. Pivot on MITRE ATT&CK Intrusion Sets, Techniques, Tools and more.

Featured



Blockchain.info (Bitcoin)

by Paterva

For visualizing the Bitcoin blockchain.



LittleSis

by Maltego Labs

Who-knows-who at the heights of business and government.

Labs



OCCRP Aleph

by Maltego Labs

Transforms for the OCCRP's Aleph instance.

Labs



Shodan

by Maltego Technologies

Shodan is the world's first search engine for Internet-connected devices. Query global IoT ...

New



Shodan (Deprecated)

by Paterva

Query Shodan data from within Maltego!



Social Links CE

by Social Links

Free transforms (No API Key required) to retrieve data from ZoomEye, Shodan, SecurityTrails, ...



SSL Certificate Transforms

by Maltego Technologies

Includes Transforms related to SSL/TLS certificates, including live certificate retrieval and ...



Wayback Machine

by Maltego Technologies

The Wayback Machine Transforms allow you to browse snapshots and archived content of hundreds of billions of websites, going back for ...

[REFRESH]

[DETAILS]

[UNINSTALL]

Installing Transforms

For our investigations, install the following transforms:

- WayBackMachine
- Standard Transforms
- Blockchain.info
- TinEye
- OCCRP Aleph
- IP Quality Score
- LittleSis

Transforms For Journalism

Maltego Transform Hub

Maltego Classic Eval - License active until 14 Jul 2022

[REFRESH] [UPDATE] ⓘ

58 Hub items total | 19 Hub items installed (1608 Transforms)

Blockchain	Infrastructure	Web Content	Bring your own key	Anti-terrorism	Incident Response	Maltego Labs
Breaches and Leaks	Malware		Data bundle	CERT	<input checked="" type="checkbox"/> Investigative Journalists	
Company Data	NLP		Free	Compliance	KYC and Corporate Investigations	
Cybersecurity	Person of Interest		Free trial	Cryptocurrency Fraud	Procurement	
Deep and Dark Web	Phishing		Paid connector	Cyber and Digital Forensics	Red Team / Pentesters	
Financial Data	Social Media			Cybercrime	SOC	
Geospatial	Threat Intelligence			Financial Crime	Trust and Safety	

TRANSFORM HUB PARTNERS 32/58 shown

Standard Transforms by Maltego Technologies

Free Standard OSINT Transforms

New

CaseFile Entities by Paterva

Additional entities from CaseFile

AliasDB by ShadowDragon

Database of Defacements and the Aliases that took attribution

ATT&CK – MISP by MISP Project

Query data from MISP. Pivot on MITRE ATT&CK Intrusion Sets, Techniques, Tools and more.

Blockchain.info (Bitcoin) by Paterva

For visualizing the Bitcoin blockchain.

CipherTrace by CipherTrace

Cryptocurrency forensics and anti money laundering (AML) intelligence.

Clearbit by Christian Heinrich

Enrich sign-ups, identify prospects and gain customer insights

dataprovider.com by dataprovider.com

Dataprovider.com transforms the internet into a structured database that lets you find ...

DomainTools Enterprise by DomainTools

Investigate cybercrime with DomainTools historic and reverse datasets.

DomainTools Iris by DomainTools

Investigate and pivot domains, identities, IPs, & more with DomainTools Iris.

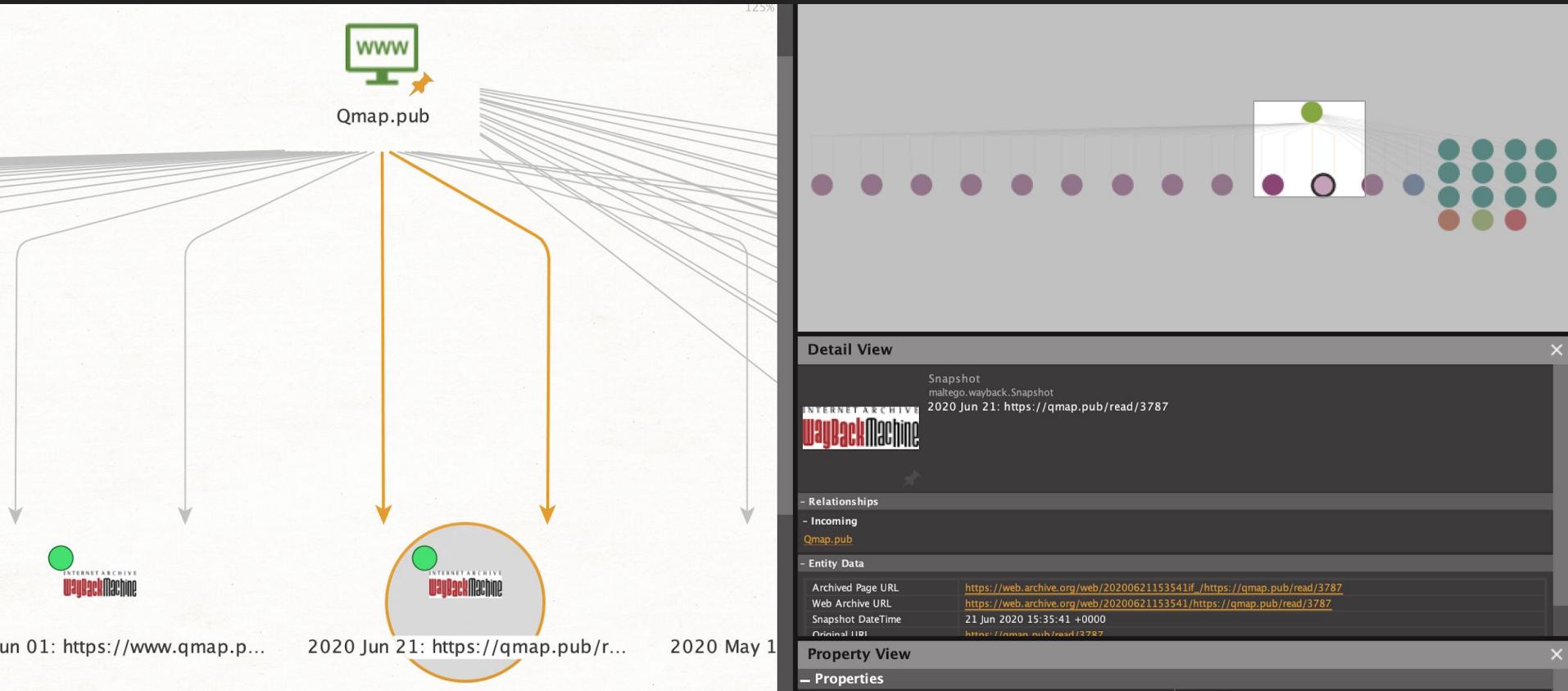
Farsight DNSDB by Farsight Security, Inc

Query the largest DNS Intelligence database, 100+ Billion records.

FullContact by Christian Heinrich

360 insights into the people who matter most.

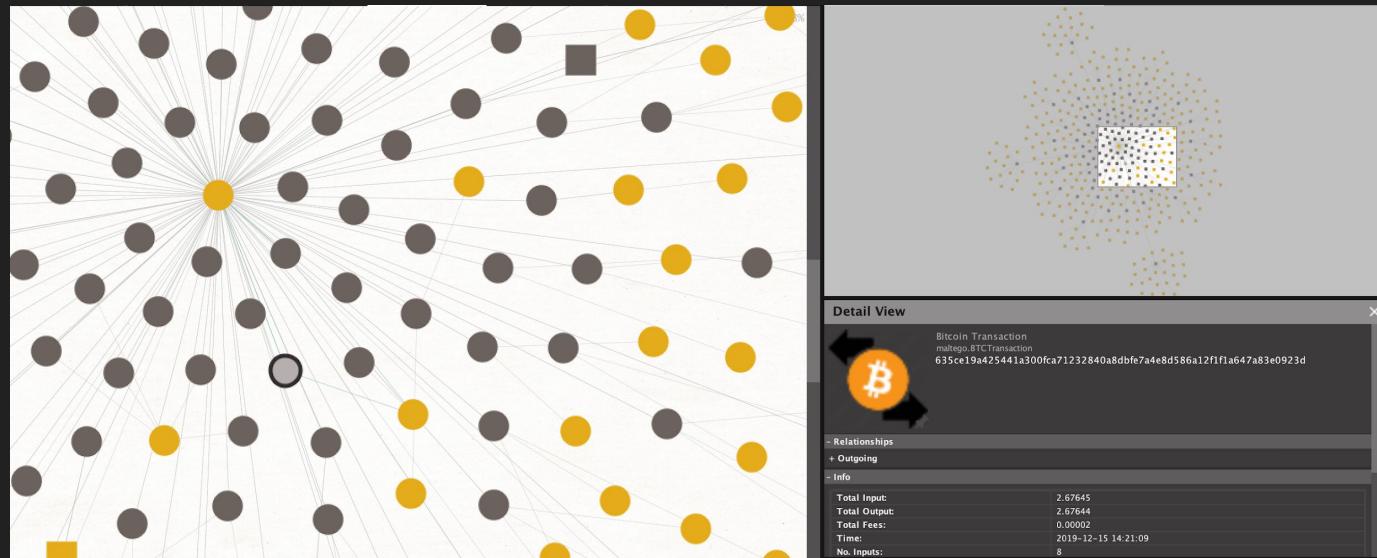
Deleted Website Investigations



Bitcoin Investigations

Criminal organizations and extremist groups often use Bitcoin to solicit donations.

Using blockchain transforms, we can identify patterns in these organizations moving money and soliciting donations.



Investigating a Bitcoin Wallet

This neo-nazi organization accepts donations via Bitcoin.

If we want to investigate their donations, and where the money goes, we can use Maltego do to this.

Nordfront now accepts donations in cryptocurrencies!



Of The editorial staff ,2018-01-25
redaktionen@nordfront.se

12

NORTH FRONT. It is now possible to donate money to Nordfront via several different cryptocurrencies and we urge Swedish nationalists to familiarize themselves with this new phenomenon.



Ethereum

Maltego currently doesn't support ethereum, but we can use a browser based tool to identify how much this contributes to their fundraising.

<https://etherscan.io>

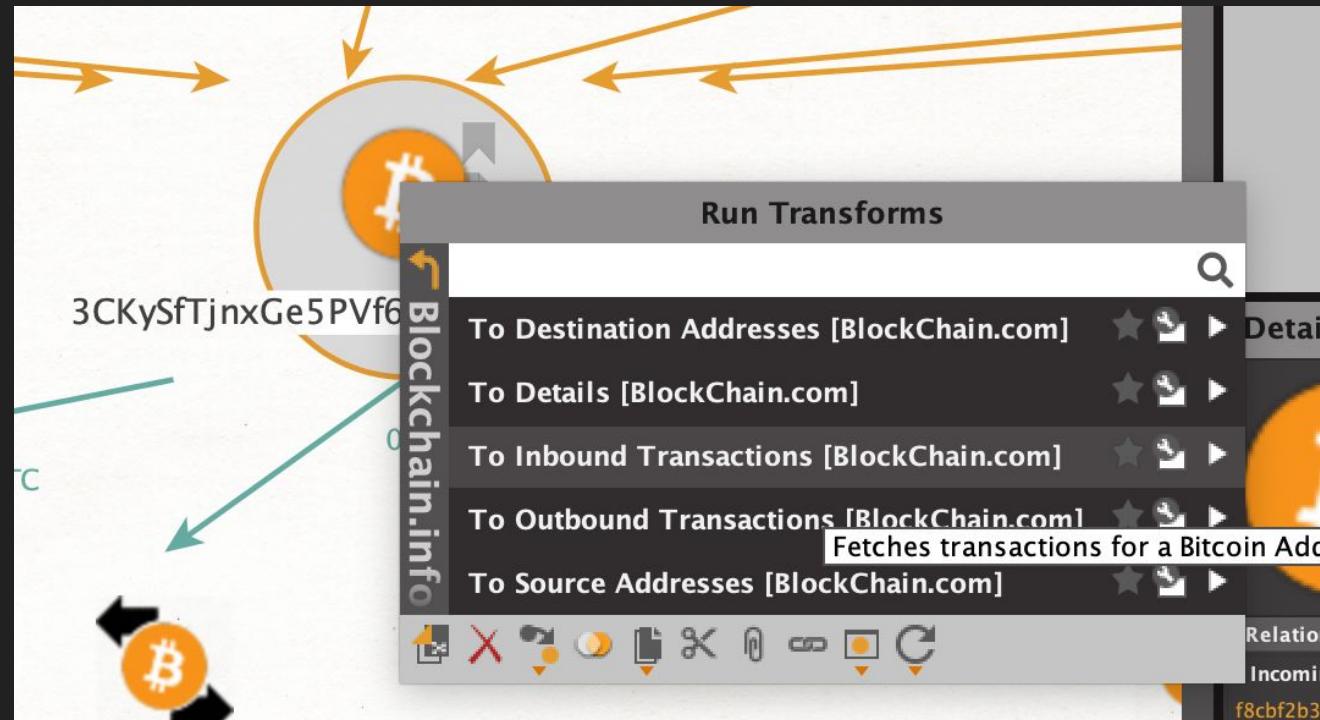
The screenshot shows the Etherscan.io interface for the Ethereum address 0x3C782B99cf0d616301748E9001ff1930C62f1428. The top navigation bar includes 'All Filters', a search bar, and links for Home, Blockchain, Tokens, Resources, More, Sign In, Buy, Exchange, Earn, and Crypto Credit. The main section is divided into 'Overview' and 'More Info'. The Overview table shows Balance (0.2691379685627816 Ether), Ether Value (\$120.30), and Token (\$16.55). The More Info section shows 'My Name Tag' as 'Not Available' with a link to update. Below these are tabs for Transactions, Erc20 Token Txns, Loans, Analytics, and Comments. The Transactions table lists 11 recent transactions, each with Txn Hash, Block, Age, From, To, Value, and Txn Fee. Notable entries include a transfer to Nanopool and several transfers to Kraken 4.

Txn Hash	Block	Age	From	To	Value	Txn Fee
0x3824331055a7e8bff...	11218430	1 day 8 hrs ago	Nanopool	0x3c782b99cf0d61630...	0.0488379685627816 Ether	0.0006321
0x73c51b6631c77039a...	10360626	133 days 14 hrs ago	0x1484d45d8f6bb8f37...	0x3c782b99cf0d61630...	0.005 Ether	0.0012705
0x30423fe320739ddca...	10356228	134 days 7 hrs ago	0x1484d45d8f6bb8f37...	0x3c782b99cf0d61630...	0.005 Ether	0.000735
0x411299f6df793b961...	10350069	135 days 5 hrs ago	0x1484d45d8f6bb8f37...	0x3c782b99cf0d61630...	0.01 Ether	0.00097125
0xb1b998292c70a567...	8878311	370 days 11 hrs ago	0x6fc1a7e46a6910f094...	0x3c782b99cf0d61630...	0.2 Ether	0.000063
0x0369392d74467271...	8344751	454 days 4 hrs ago	0x96dcfd084da25ec6...	0x3c782b99cf0d61630...	0.0003 Ether	0.00021
0xff86b9e99f43546184...	7580156	573 days 9 hrs ago	0x3c782b99cf0d61630...	0xe716d9a51b7f11aa5...	2.172544099854376 Ether	0.0006589
0x80611dfa9c73f6cd7...	7521935	582 days 10 hrs ago	0x59a52c24d8a631405...	0x3c782b99cf0d61630...	2 Ether	0.00021
0x11e7b75797b9cbfb0...	6211310	807 days 12 hrs ago	0x38743ca36809f65cf1...	0x3c782b99cf0d61630...	0.15 Ether	0.000462
0xb9ecdcb272768f2c4b...	6184508	812 days 1 hr ago	0x1484d45d8f6bb8f37...	0x3c782b99cf0d61630...	0.018202999854376 Ether	0.0000470799
0xdaf06214667d5a9ac...	5861781	866 days 20 hrs ago	Kraken 4	0x3c782b99cf0d61630...	0.005 Ether	0.00063

Identifying Incoming Transactions

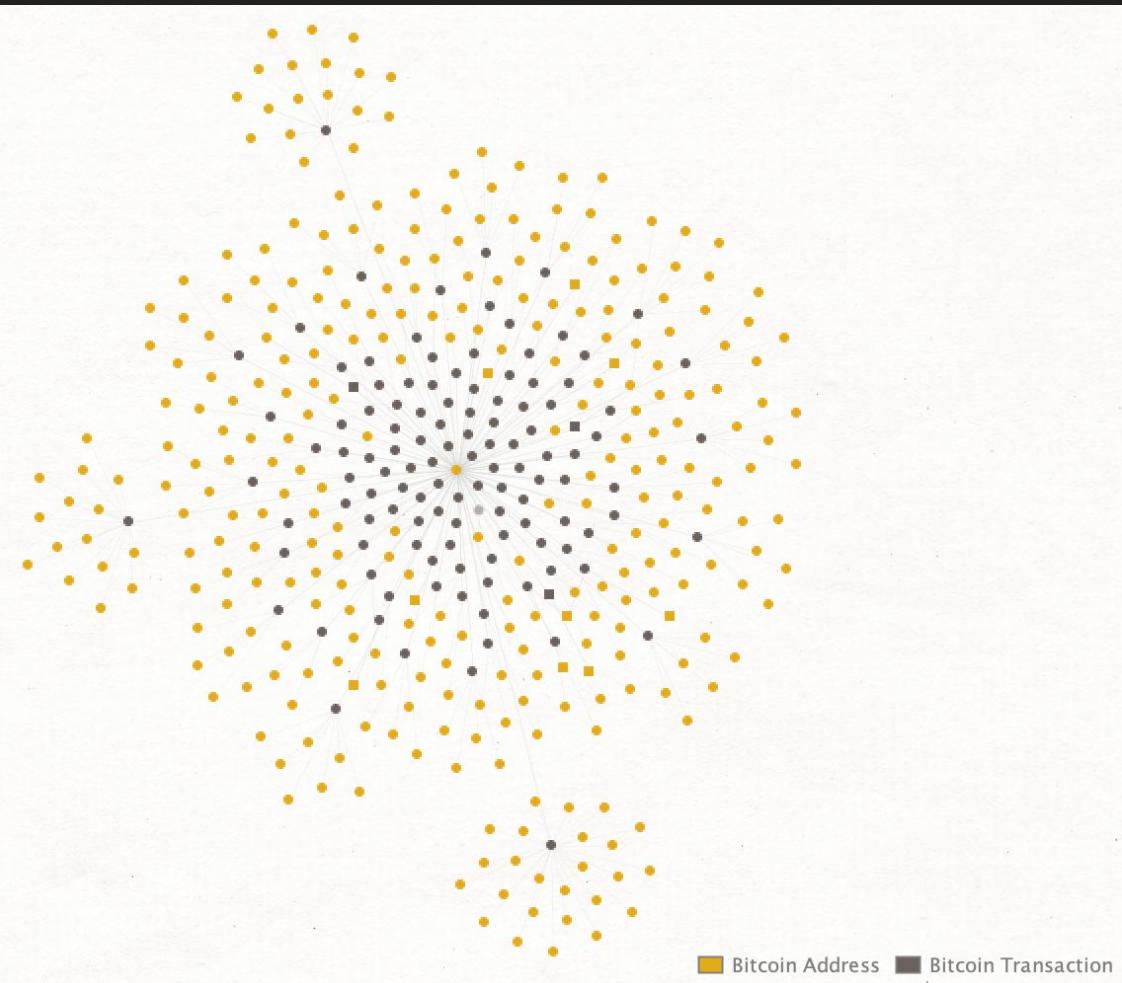
We can create a bitcoin wallet entity, and add the address of our target.

Then, we run the “inbound transactions” transform to show payments to this wallet.



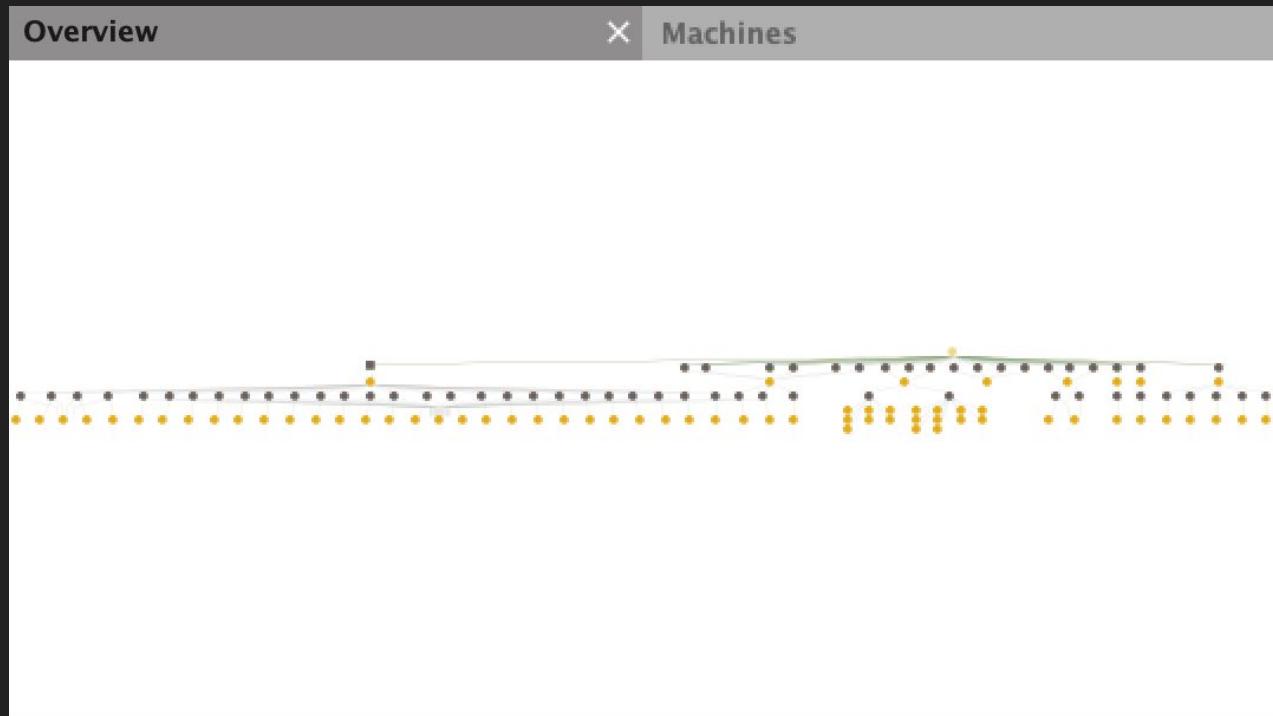
Incoming Donations

By adjusting the layout, we can make it easier to see patterns.



Where Does The Money Go?

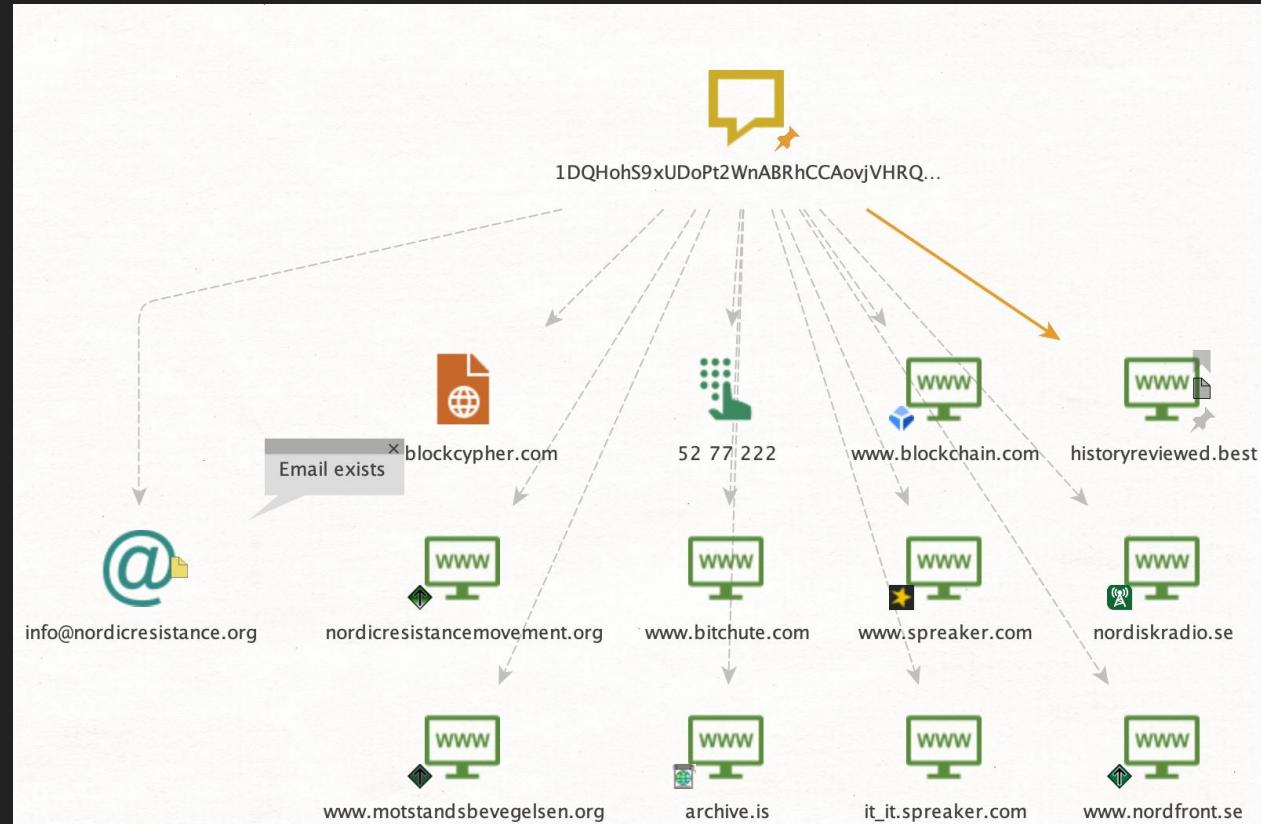
Looking at outbound transactions, and going one layer deep, we can find more information about where the money is going.



Identifying Fundraising Efforts

To identify where the wallet address is raising money, we can make a “phrase” entity, and paste the Bitcoin wallet address into it.

Here, we find media outlets of the organization raising money with the wallet ID.



Identifying Social Channels

We have identified a media funding effort of the organization, this one calling for journalists to be hung on lamp posts.

We find an address we can use to find more information, and playlists full of their media content.

It also includes some social media handles we can use to further investigate.

NORDIC FRONTIER #126: IMPORTING AIDS

WATCH



First published at 10:58 UTC on November 19th, 2019.



NRM Radio

Nordic Frontier

466 subscribers



DONATIONS:

For those of you who would like to support our movement by sending us cash in the mail, you can send it to this address:

Nordfront
Box 52
77222 Grängesberg
Sweden

Bitcoin (BTC): [1DQHohS9xUDoPi2WnABRhCCAovjVHRQv4d](https://www.blockchain.com/btc/address/1DQHohS9xUDoPi2WnABRhCCAovjVHRQv4d)

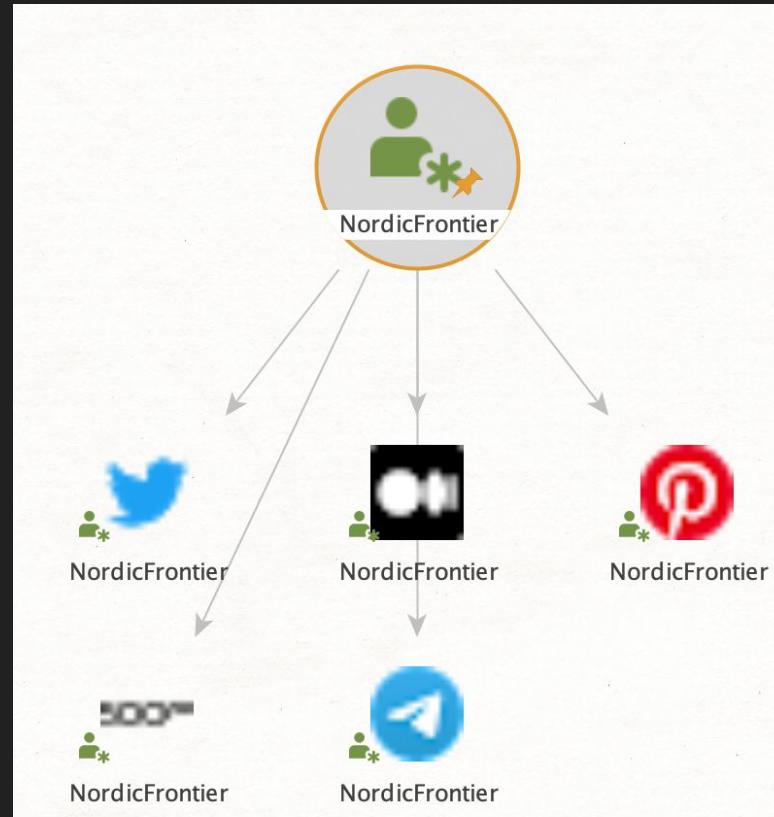
Category News & Politics

Sensitivity Normal - Content that is suitable for ages 16 and over

Locating Social Media Accounts

From the name of the media account, we create an “alias” entity, and run a search for social media accounts.

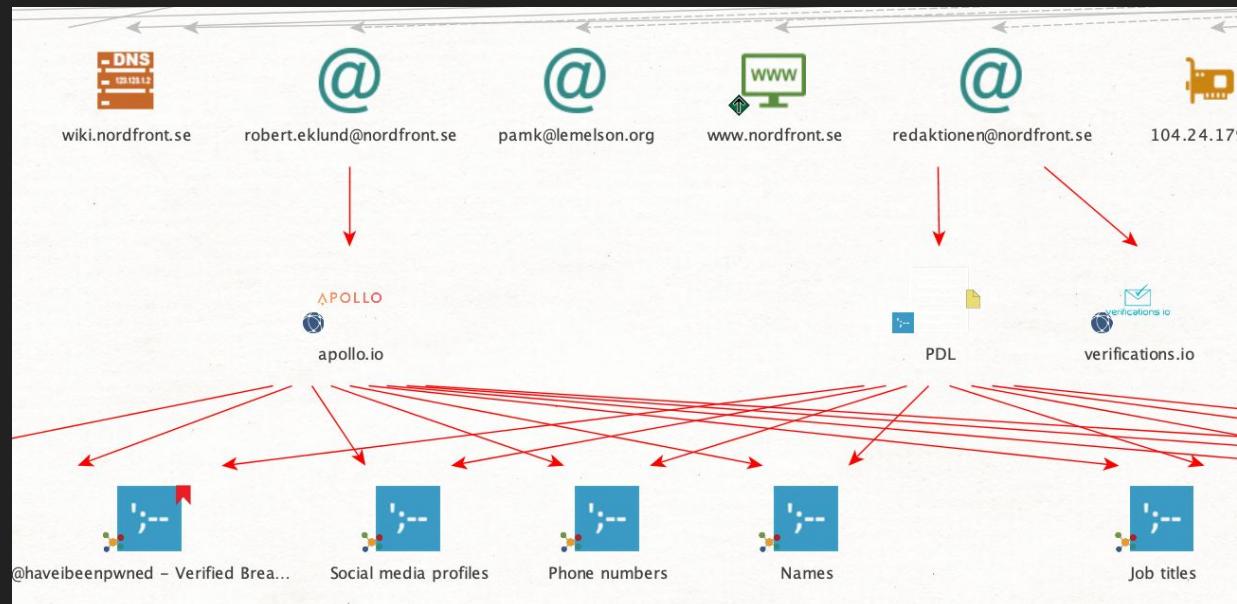
We find more social media accounts from the organization.



Finding Account Breaches

By using email addresses found from theHarvester, we can discover if any have been breached.

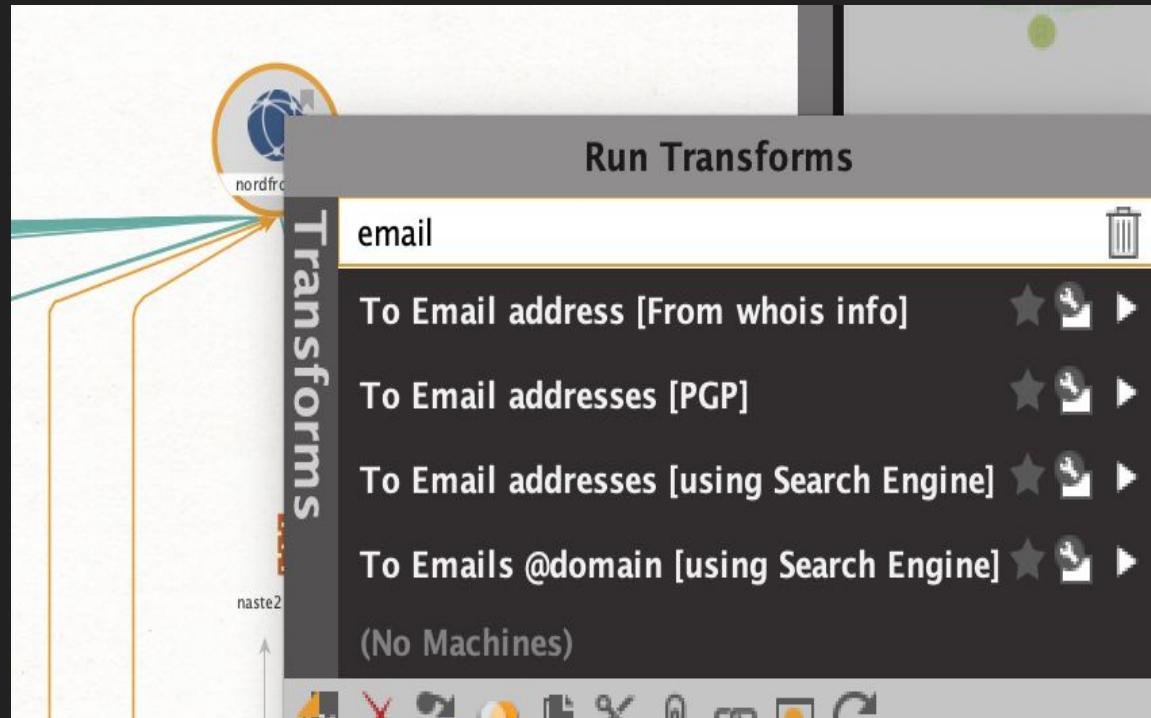
We can also find email addresses from the domain in Maltego.



Identify Email Addresses

First, create a domain entity, and add the domain name of the target.

Using the “To Emails @domain” transform, identify other email addresses from the target domain.



Look for Email Breaches

Select the discovered email addresses.

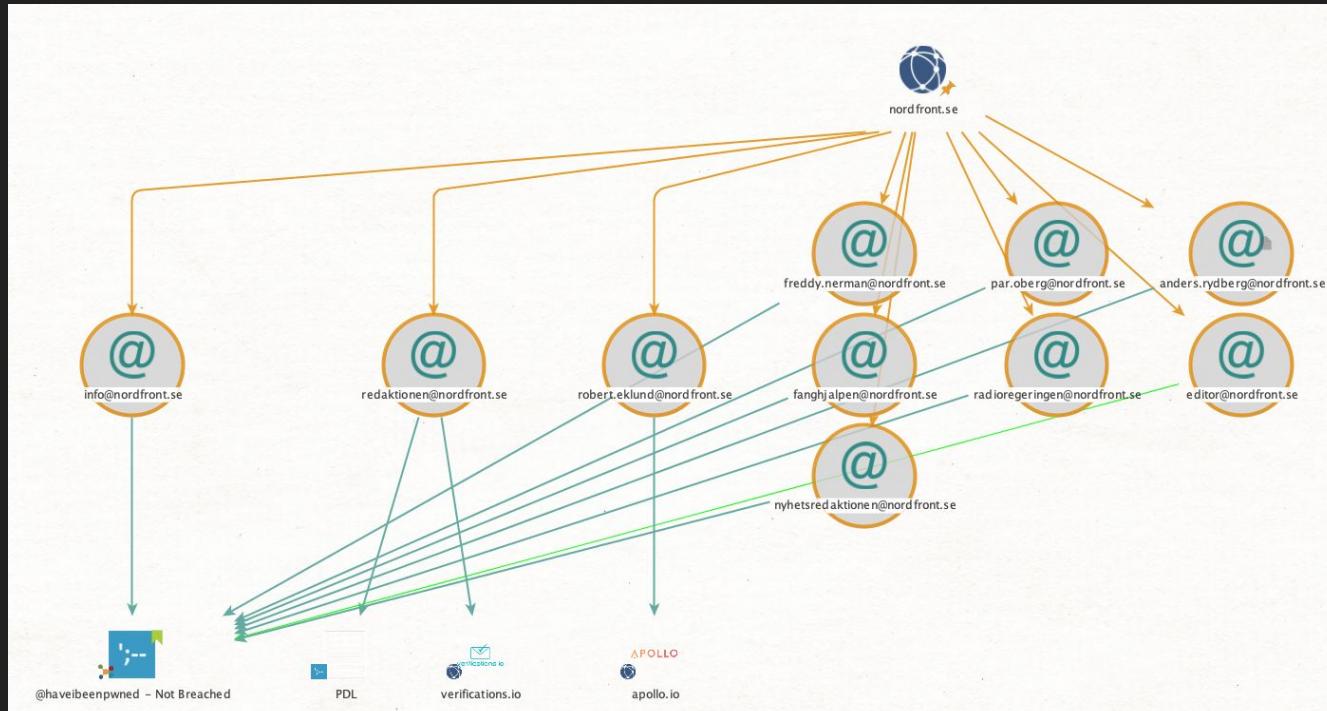
Then, run the “**get all breaches of an email address**” transform from “**have I been pwned**” transform set.



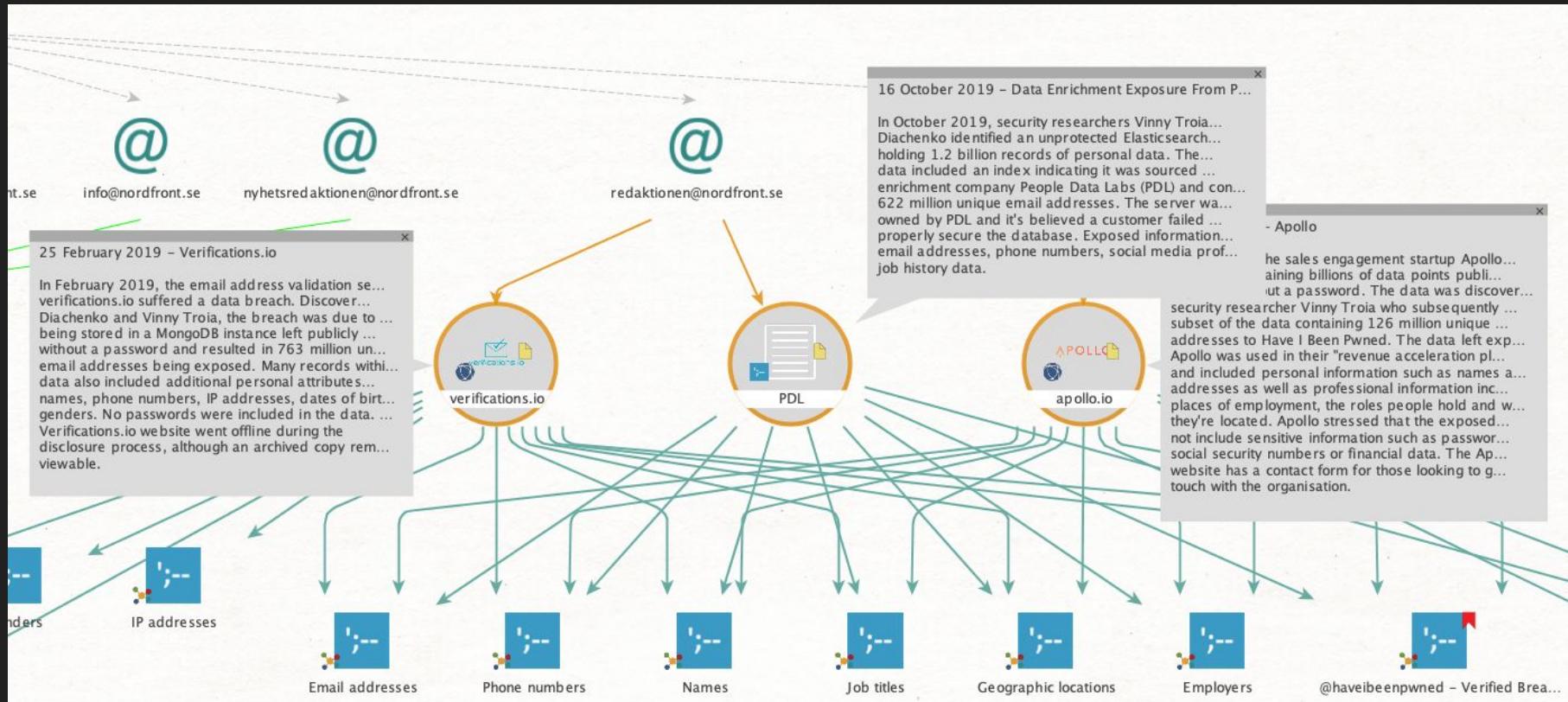
Sorting Through Results

If email addresses were not breached, they will point to a “not breached” entity.

If they are breached, the breach they were involved in will be shown on the screen



Enrich Breach Data



Practice!

I've given some examples of how to identify email addresses associated with an organization, and how to identify data breaches. Can you:

- Identify other email addresses at a target organization?
- Find an email account that has been breached on that list?
- Find an account breach that involved passwords?

As a bonus:

- Locate a business accepting payment to a Bitcoin wallet
- Identify the total number of customers
- Identify payments from the target wallet to other wallets