WETENSCHAP
EN TECHNIEK

AP HOGESCHOOL
ANTWERPEN

Magnum Opus

Maltego CE / CaseFile

Imad El-Azzouzi

(ter informatie alle informatie die ik heb gevonden worden niet misbruikt)

(normaal zou ik enkel CaseFile gebruiken maar dit is enkel voor het offline gebeuren daarom zal ik Maltego CE (hier gebeurd alles automatisch) en CaseFile gebruiken, verder meer info)

https://paterva.com/buy/maltego-clients/maltego-ce.php

Maltego

is een interactieve tool voor datamining die gerichte grafieken weergeeft voor linkanalyse. De tool wordt gebruikt in online onderzoeken voor het vinden van relaties tussen stukjes informatie uit verschillende bronnen op internet.

Maltego gebruikt het idee van transformaties om het proces van het doorzoeken van verschillende gegevensbronnen te automatiseren. Deze informatie wordt vervolgens weergegeven op een op een knooppunt gebaseerde grafiek die geschikt is voor het uitvoeren van linkanalyse.

De Maltego clients hebben toegang tot een bibliotheek met standaardtransformaties voor de ontdekking van gegevens uit een breed scala aan openbare bronnen die vaak worden gebruikt in online onderzoeken en digitale forensisch onderzoek.

Omdat Maltego naadloos kan worden geïntegreerd met vrijwel elke gegevensbron, hebben veel gegevensverkopers ervoor gekozen om Maltego te gebruiken als een leveringsplatform voor hun gegevens. Dit betekent ook dat Maltego kan worden aangepast aan uw eigen, unieke vereisten. Onze huidige datapartners zijn te vinden op de Transform Hub-pagina waarnaar hieronder wordt gelinkt.

Focus of Maltego

Het analyseren van real-world relaties tussen informatie die publiek toegankelijk is op internet, dit omvat footprinting internetinfrastructuur en het verzamelen van informatie over de mensen en organisatie die er eigenaar van zijn.

Gebruik

om de relaties tussen de volgende entiteiten te bepalen:

- People.
    - Names.
    - Email addresses.
    - Aliases.
- Groups of people (social networks).
- Companies.
- Organizations.
- Web sites.
- Internet infrastructure such as:
    - Domains.
    - DNS names.
    - Netblocks.
    - IP addresses.

- Affiliations.
- Documents and files.

The Transform hub

What is the Transform hub?

De Transform Hub is in elke Maltego-client ingebouwd en stelt gebruikers van Maltego in staat om gemakkelijk transformaties te installeren die door verschillende gegevensproviders zijn gebouwd. De Transform Hub is verdeeld tussen commerciële en community (gratis) transformaties.

Reden: *De flexibiliteit van Maltego als het gaat om de integratie van externe gegevens heeft ertoe geleid dat veel gegevensverkopers ervoor hebben gekozen om Maltego te gebruiken als een platform voor gegevenslevering voor hun gebruikers.*

Hieronder vindt u details over de verschillende transformatieproviders die ik heb gebruikt

- Haveibeenpwnd: een website waarmee internetgebruikers kunnen controleren of hun persoonlijke gegevens zijn aangetast door datalekken. Hierin vond ik dan stockx.com en andere websites.
- The movie database: om namen van films, talent en regisseurs te zoeken en te draaien. Zeer leuke transform dat ik ook heb gebruikt in cases vindt u meer info

Kort

- Maltego kan worden gebruikt voor de informatieverzamelingsfase van alle beveiligingsgerelateerde werkzaamheden. Het bespaart u tijd en stelt u in staat om nauwkeuriger en slimmer te werken.

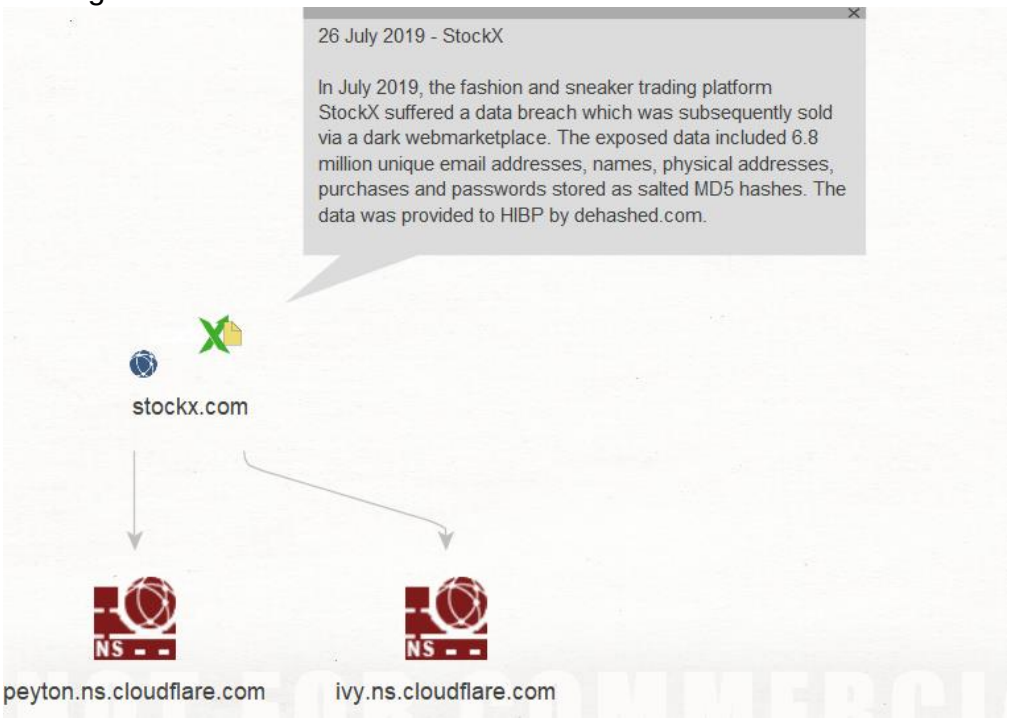
- Maltego biedt u een veel krachtigere zoekopdracht, waardoor u slimmere resultaten krijgt. Als toegang tot "verborgen" informatie uw succes bepaalt, kan Maltego u helpen deze te ontdekken.

- Maltego helpt u in uw denkproces door visueel verbonden koppelingen tussen gezochte items visueel aan te tonen.

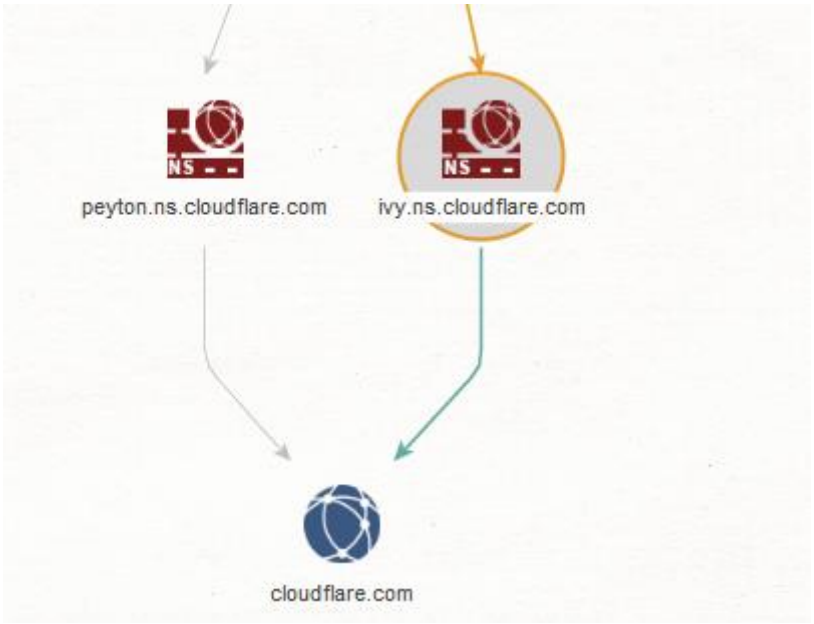
serious Cases

Case 1: *Werknemersaccounts vinden met wachtwoordbreuken met behulp van*

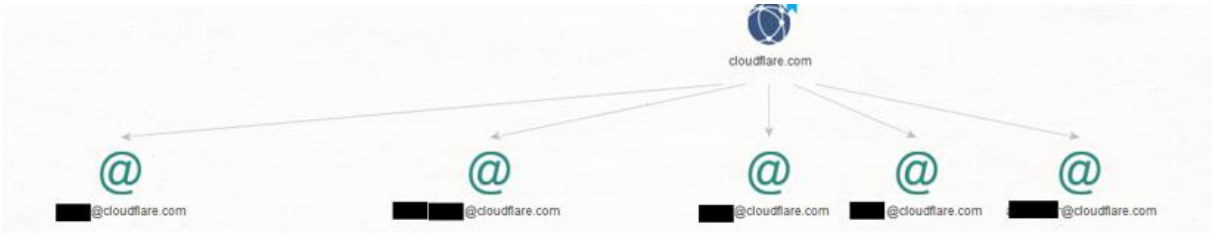
Hier zal ik een domein gebruiken die al eens is gebreached is, namelijk stockx.com.
Eerst gezocht naar de verschillende NS-Records



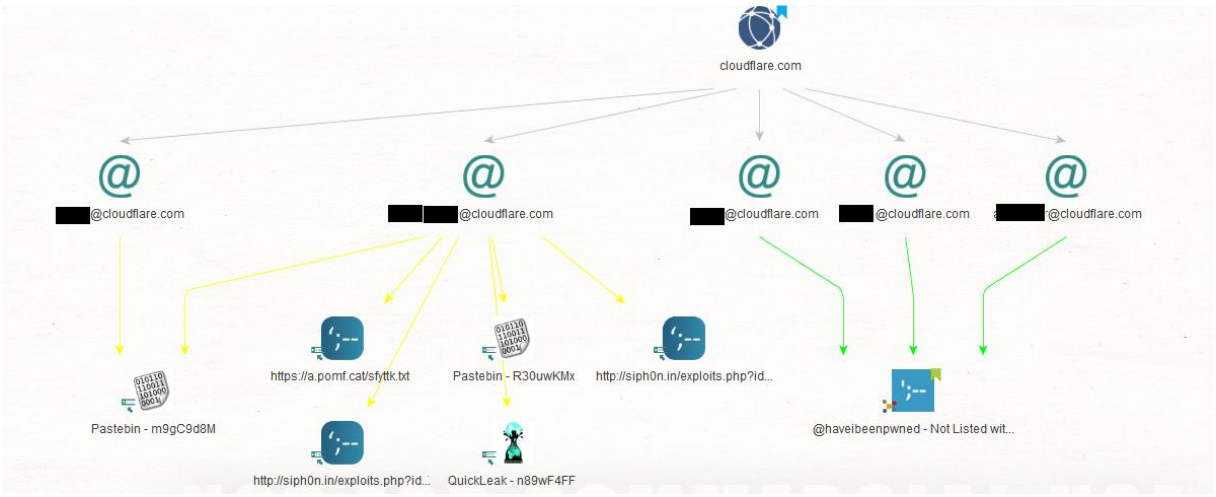
deze zet ik dan om naar een domein



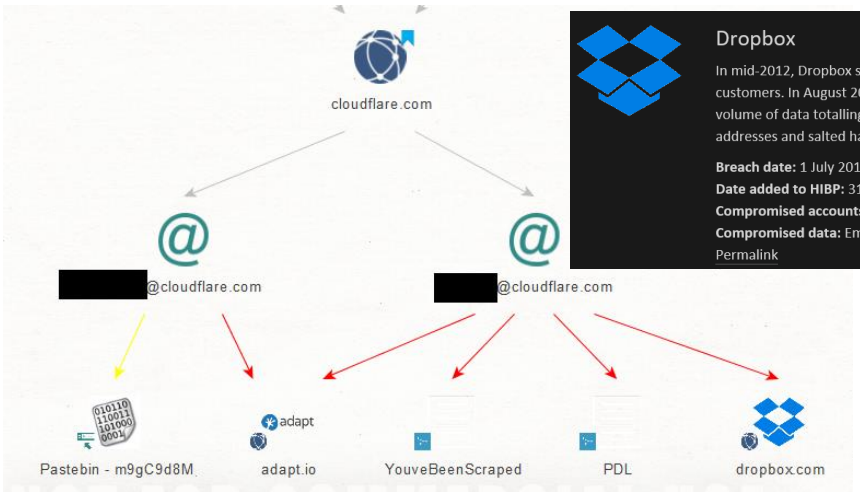
Ik haal dan alle e-mails op (sommige verwijderd want er zaten er veel te veel)

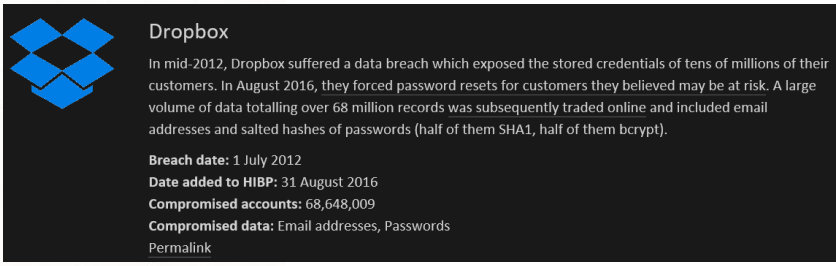


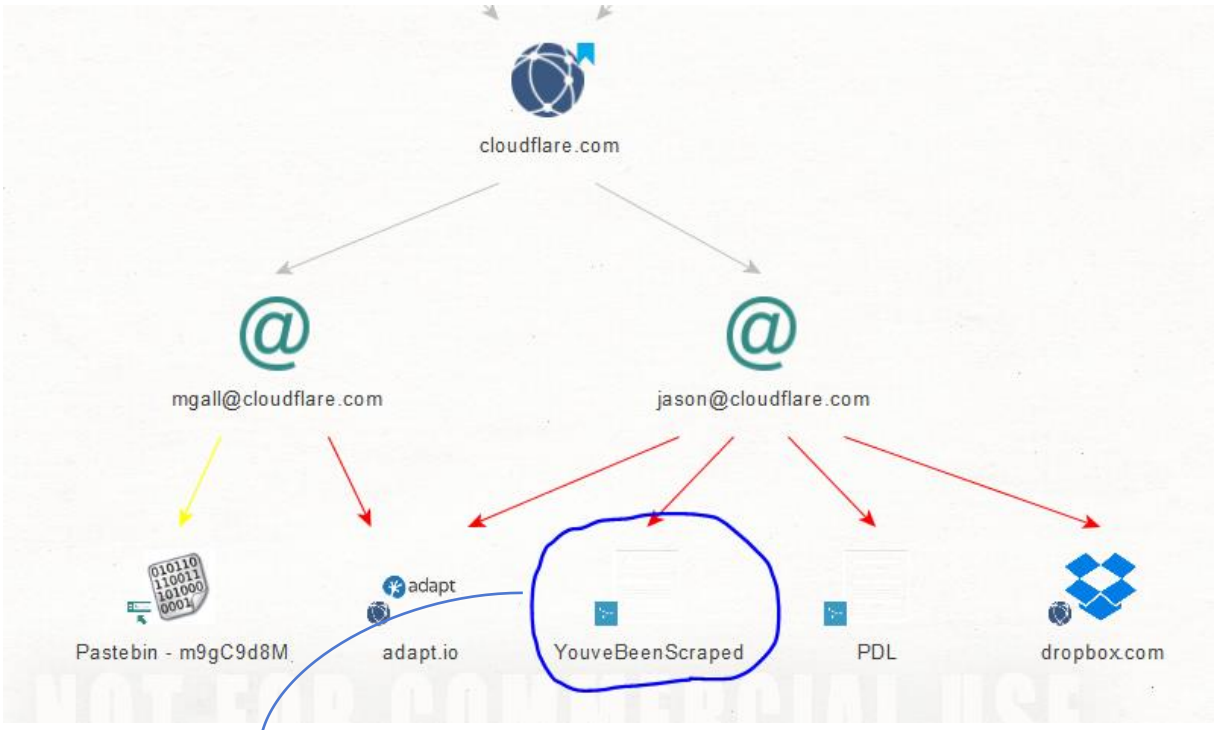
Hierna kan je veel doen, je kan de email omvormen naar een persoon en daarna meer info krijgen over die persoon, maar hier gaan we zien of de e-mails die we hebben gekregen meer info kunnen geven (Pastebin: hierin zit meer info over de e-mails (wie de user is, locatie, enz)

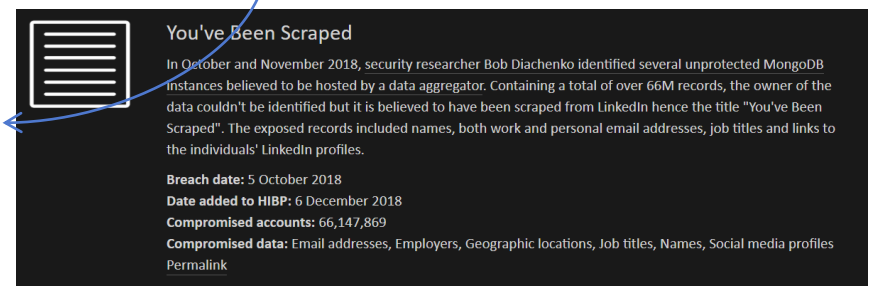


nu kan ik op elk email een onderzoek starten, maar hier zal ik 1 email nemen onderaan deze tekst heb ik een email waar veel info is over terug gegeven, de rechtse email zie je dat dropbox.com erbij staat dit wilt zeggen dat dropbox een data lek heeft meegemaakt en als ik dit zal opzoeken vinden we dit ook terug

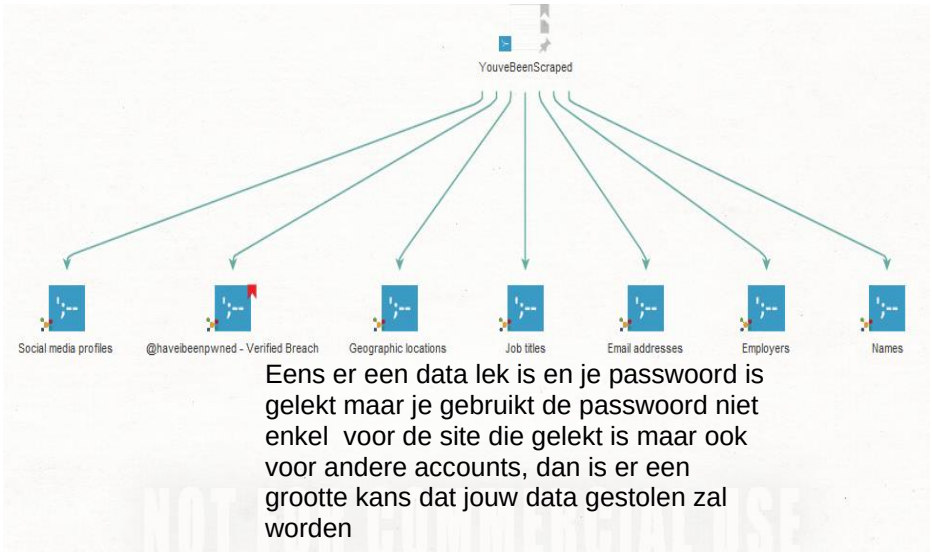




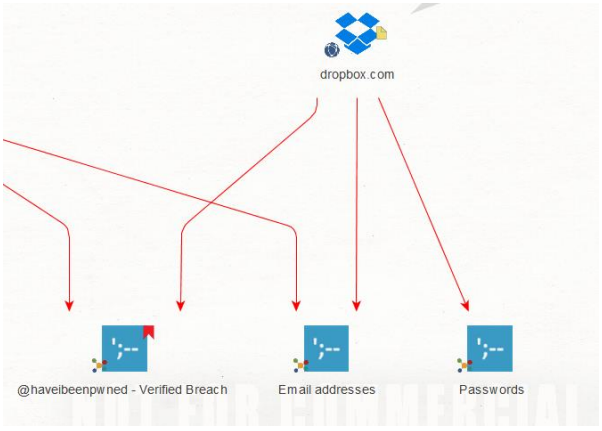




deze persoon is dan zijn informatie verloren wegens breaching van dropbox, adapt.io en you've been scraped, onderaan zie je wat de datalekken allemaal heeft veroorzaakt



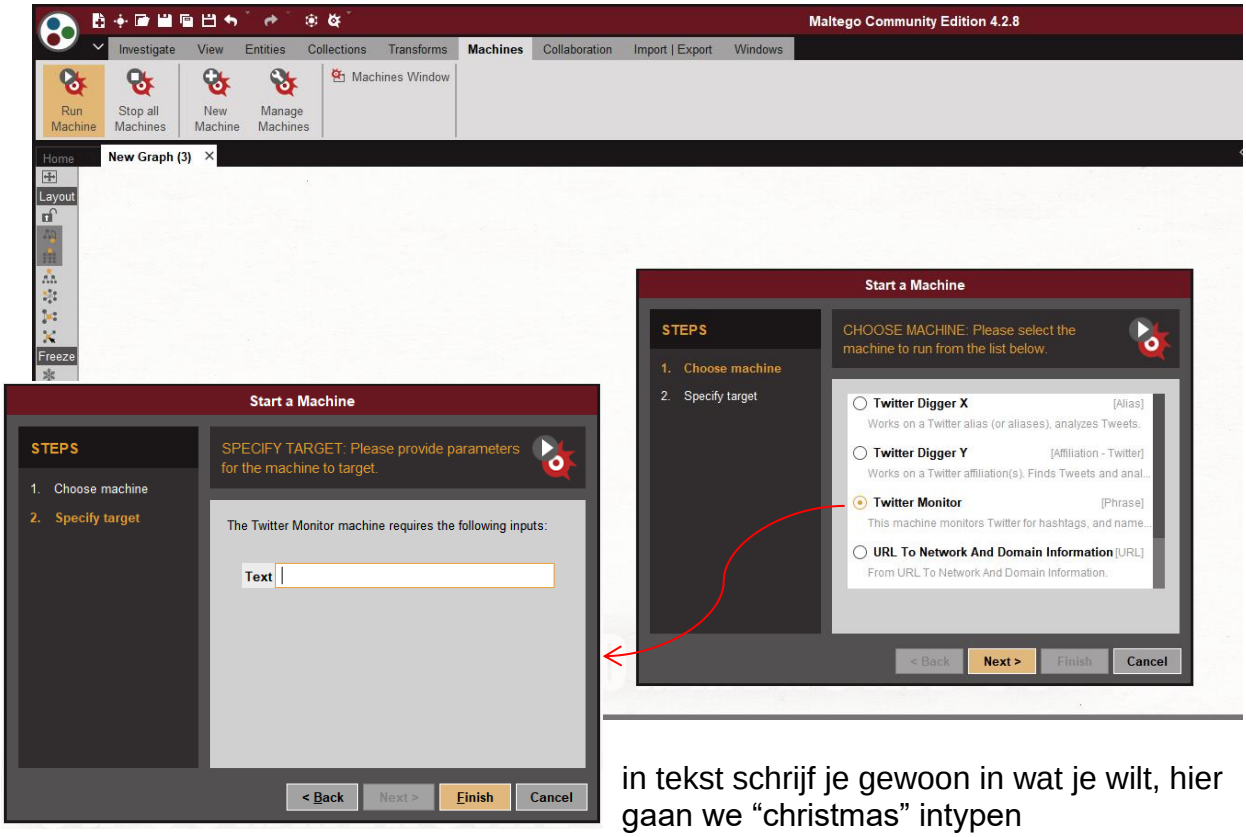
Eens er een data lek is en je password is gelekt maar je gebruikt de password niet enkel voor de site die gelekt is maar ook voor andere accounts, dan is er een grootte kans dat jouw data gestolen zal worden



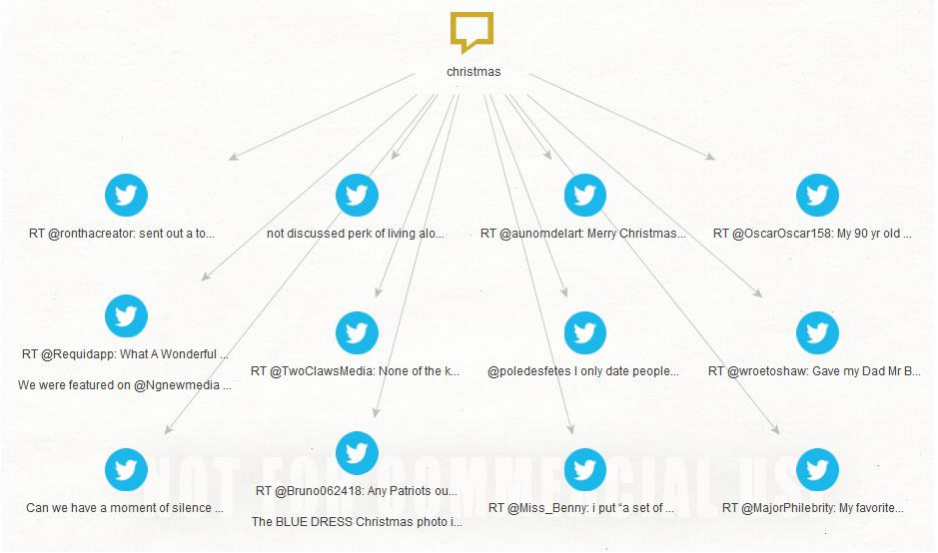
Case 2: *Hoe Live Twitter-discussies te volgen voor desinformatie-aanvallen*

hackers zijn vaak verantwoordelijk voor het monitoren en beïnvloeden van gesprekken op sociale media. De manier hoe ze dit doen is door eerst identificeren en vervolgens beginnen met het monitoren van zowel de mensen als de hashtags die worden gebruikt om informatie te verspreiden dat misschien over een politiek protest gaat

we starten door eerst een machine op te starten waar je verschillende mogelijkheden krijgt die je dan kunt uitvoeren op bepaalde entiteiten

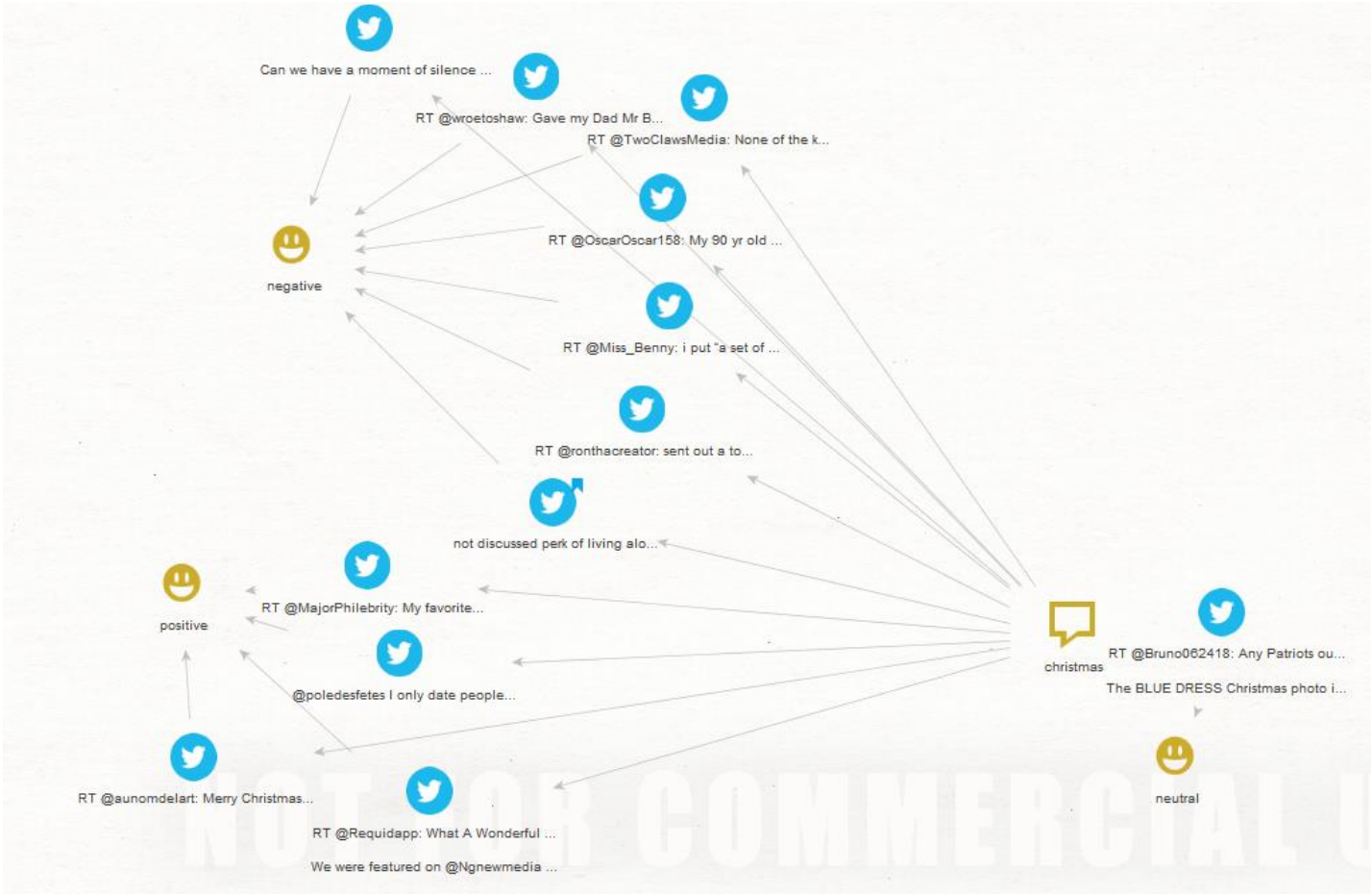


in tekst schrijf je gewoon in wat je wilt, hier gaan we “christmas” intypen



dit is wat ik heb gevonden over “christmas”

We kunnen ook nazien of de tweet negatief, positief of neutraal is zodat kan je zien of het onderwerp wel de goede of foute richting gaat, of het over iets goed of slechts gaat (het kan ook zo zijn dat in een tweet een bepaalde woord negatief is maar niet echt een negatieve tweet is, sarcasme, dit is omdat de machine (IBM Watson = Supercomputer) het verschil niet weet



laten we zeggen dat je een hacker bent die een hoop propaganda wilt verspreiden, je kunt mensen vinden die positieve of negatieve meningen over polariserende opvattingen uiten. Je kunt ook de auteurs vinden, zodat je ze kunt opvolgen door ze rechtstreeks een bericht te sturen of door de inhoud op te zoeken die ze delen

geweldige manier om op Twitter te duiken zonder de hele dag door te brengen achter de grafische UI door tweets te bladeren, omdat je hiermee informatie zoals gebruikersnaam kunt ophalen en vervolgens zoekopdrachten kunt uitvoeren om andere dingen te bepalen die ze misschien hebben gezegd of het al dan niet een goed doelwit zou zijn voor een social engineering-attack.

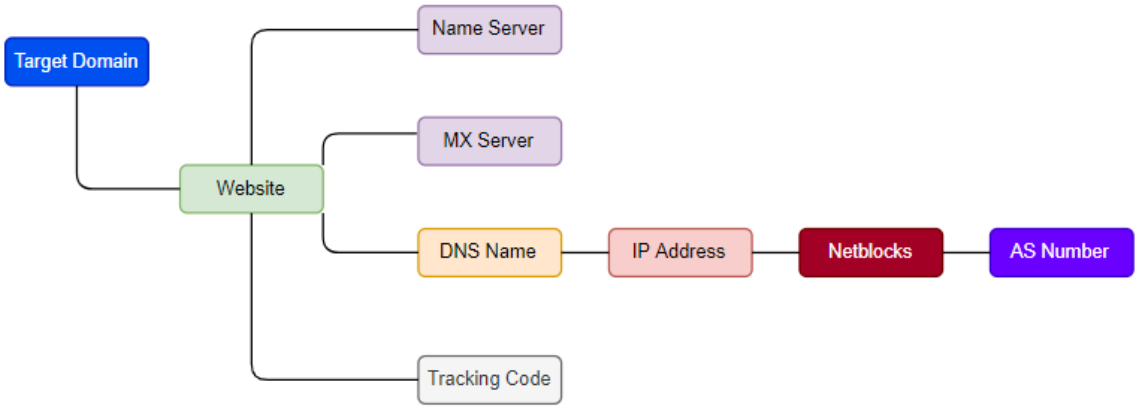
de flexibiliteit hiervan om live evenementen te monitoren en ook evenementen die in het recente verleden hebben plaatsgevonden, zijn behoorlijk indrukwekkend

Geavanceerde hardnekkige bedreigingen zoals door de staat gesteunde hackers zullen deze zwakke punten blijven gebruiken in platforms zoals Twitter die worden gebruikt voor online discussies om politieke, propaganda- en censuurambities te vervullen.

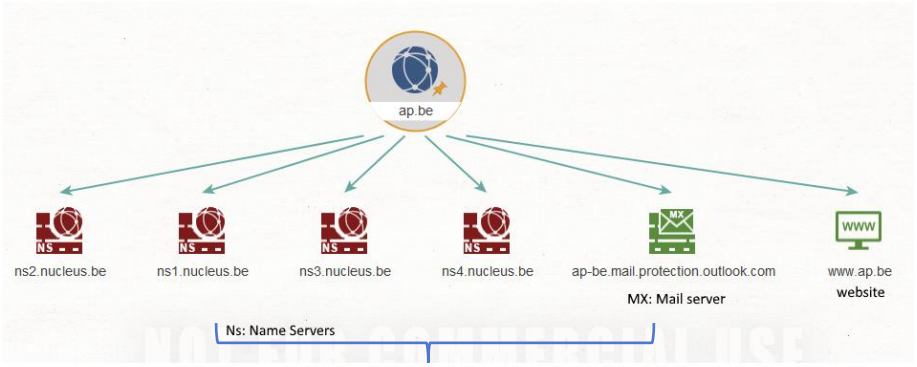
Case 3: *om een volledig netwerk af te drukken met alleen een domeinnaam*

Door alleen details te weten zoals de MX-server, kunnen we ook weten welke e-mailprovider een bedrijf gebruikt, wat een hacker een voordeel oplevert bij een phishing-aanval.

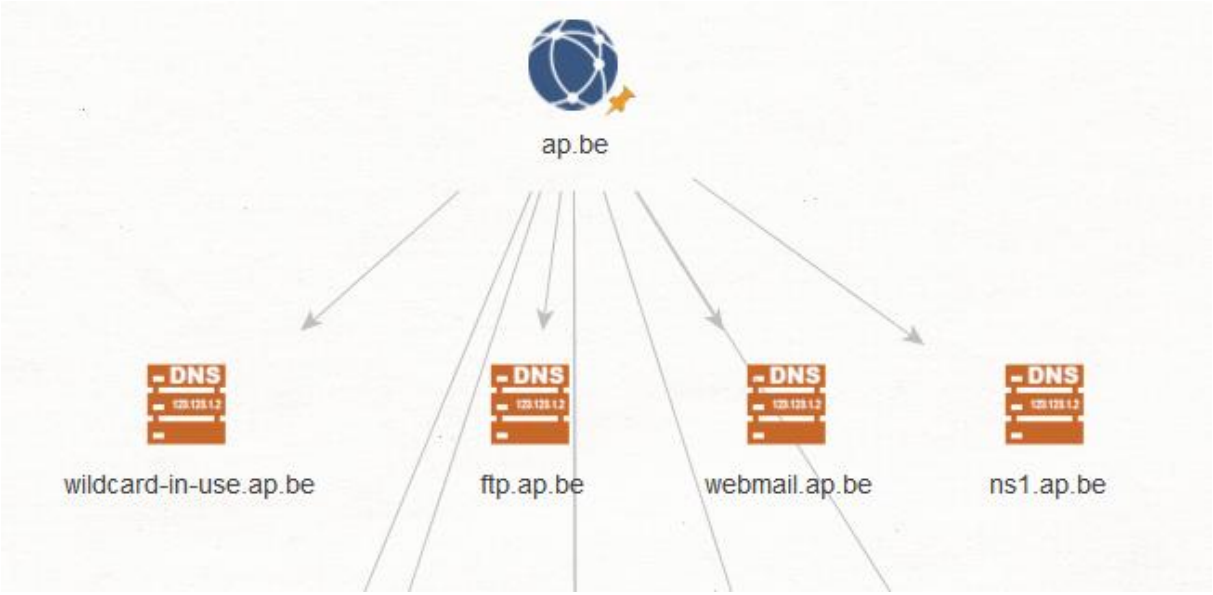
Al deze details kunnen nuttig zijn, afhankelijk van uw doelstelling en wat u van plan bent met de informatie te doen, dus laten we de keten schetsen die we gaan maken om de netwerkinfrastructuur van ons doel beter te begrijpen.

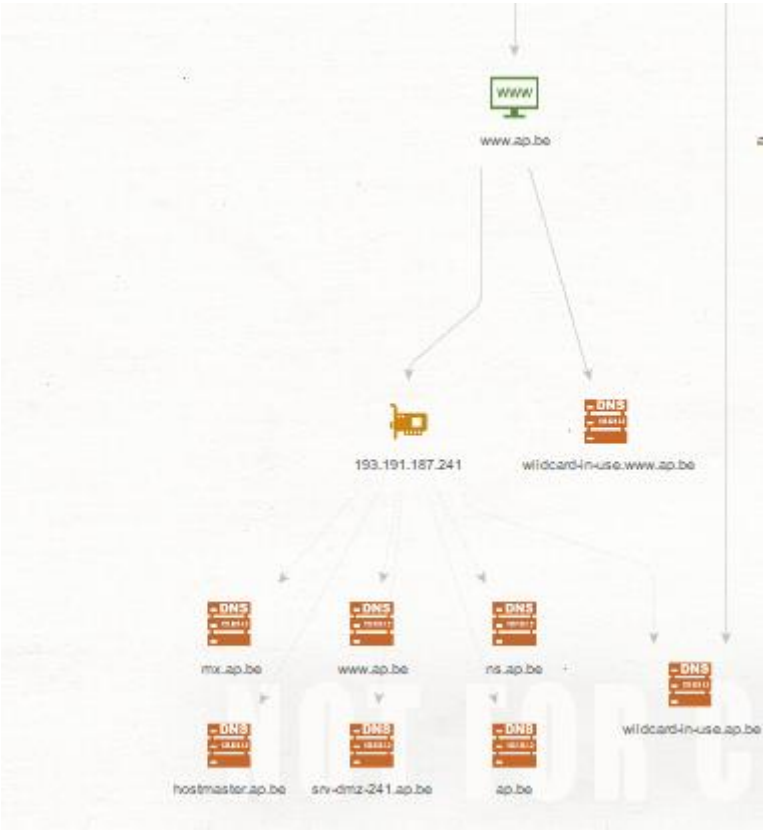


Het vaststellen van de keten van domein naar AS-nummer is nuttig om ons onderzoek georganiseerd te houden. Wanneer we helemaal naar het AS-nummer zijn, kunnen we beginnen met terugkijken op de keten en beginnen we uit te breiden naar wat we aanvankelijk hebben gevonden.



Dit zijn de “common dns names”

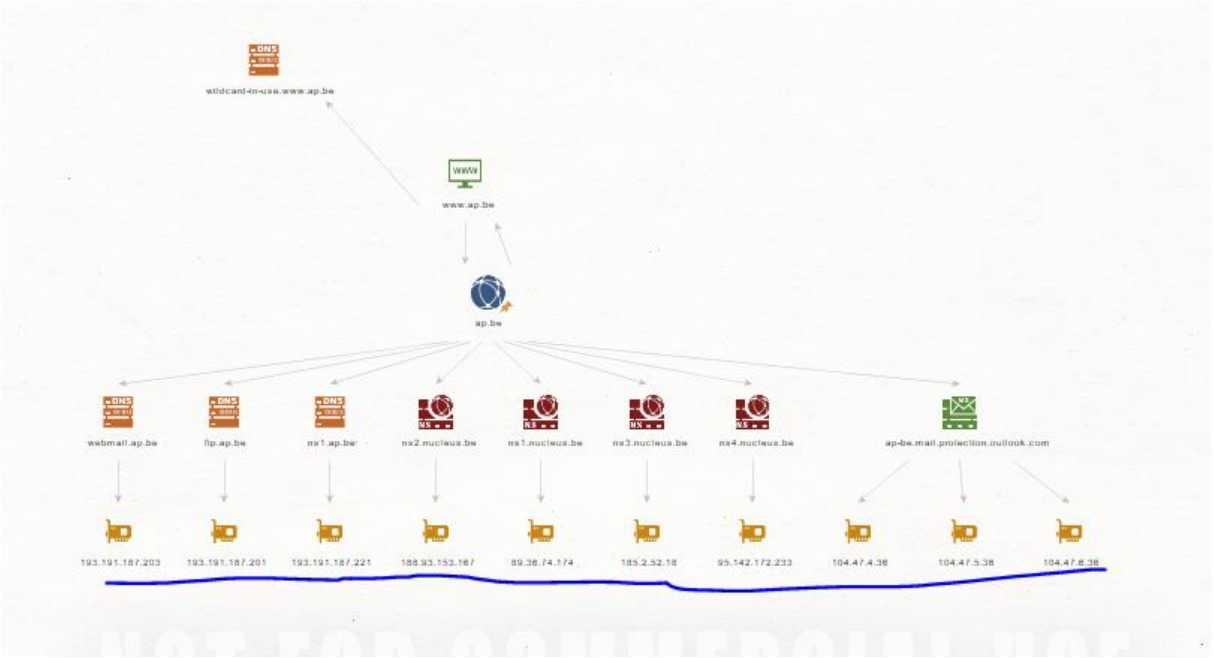




meer dns servers gevonden die op dezelfde IP Address zitten

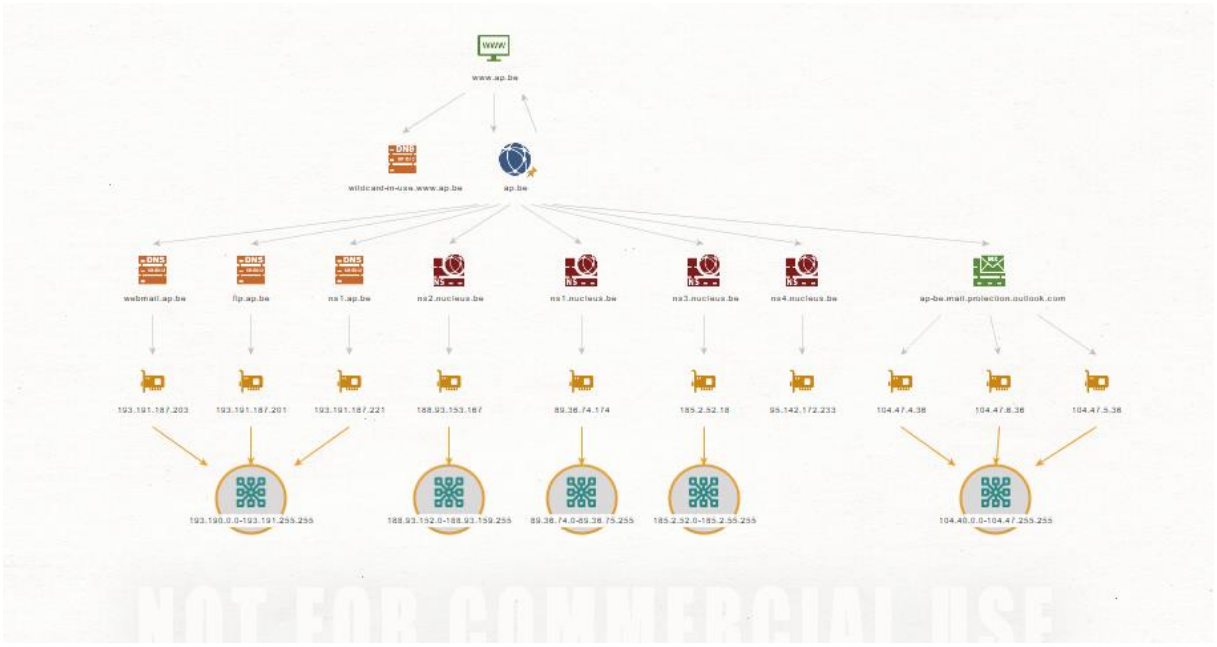
enkel van de domain heb ik al zoveel informatie kunnen verkrijgen, al deze andere dns-servers die verwijzen naar andere delen van de website waar we nog nooit van hebben geweten dankzij dit tool

In de volgende stap gaan we alle dns servers die we hebben gekregen nu de IP Address achterhalen



De volgende stap is dan om van deze IP Addresse de netblocks te krijgen

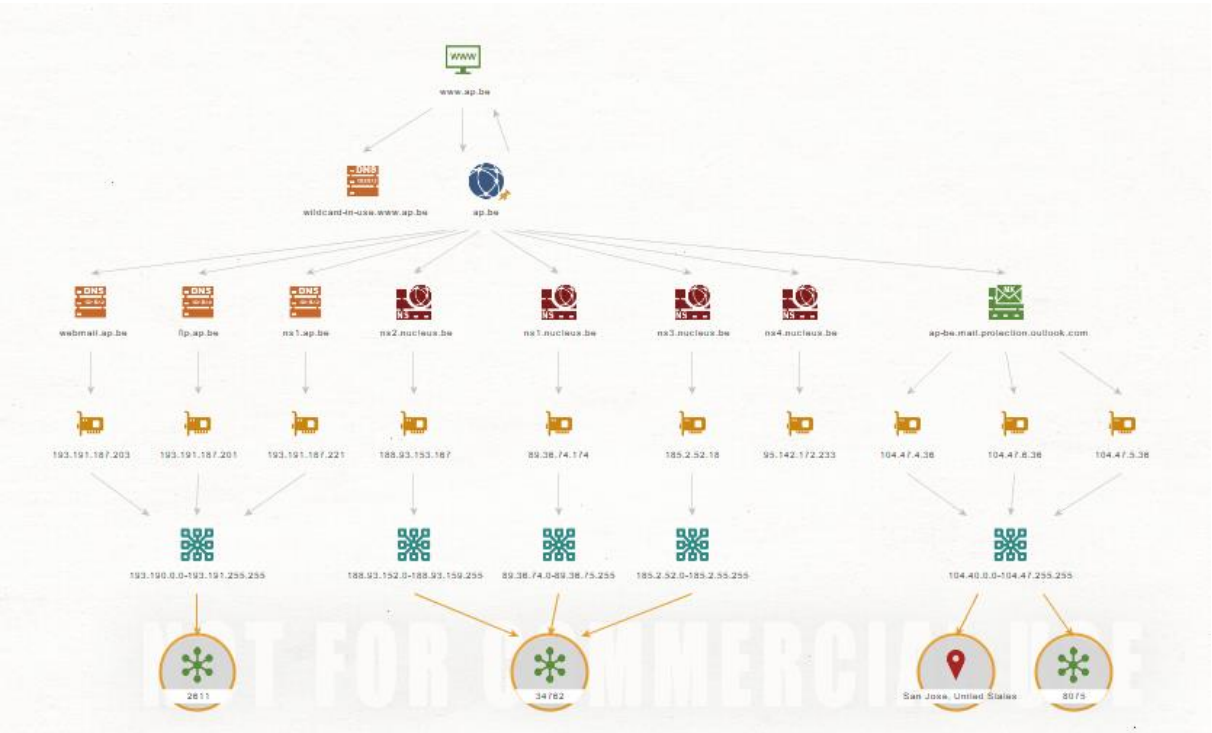
Een netblock is eigenlijk een reeks van IP-adressen die een specifieke ISP of datacenter bezit en die naar verlangen kan toewijzen. In de context van digitaal adverteren, zorgen netblock mapping-tabellen voor zaken als ISP-targeting. (thank you google)



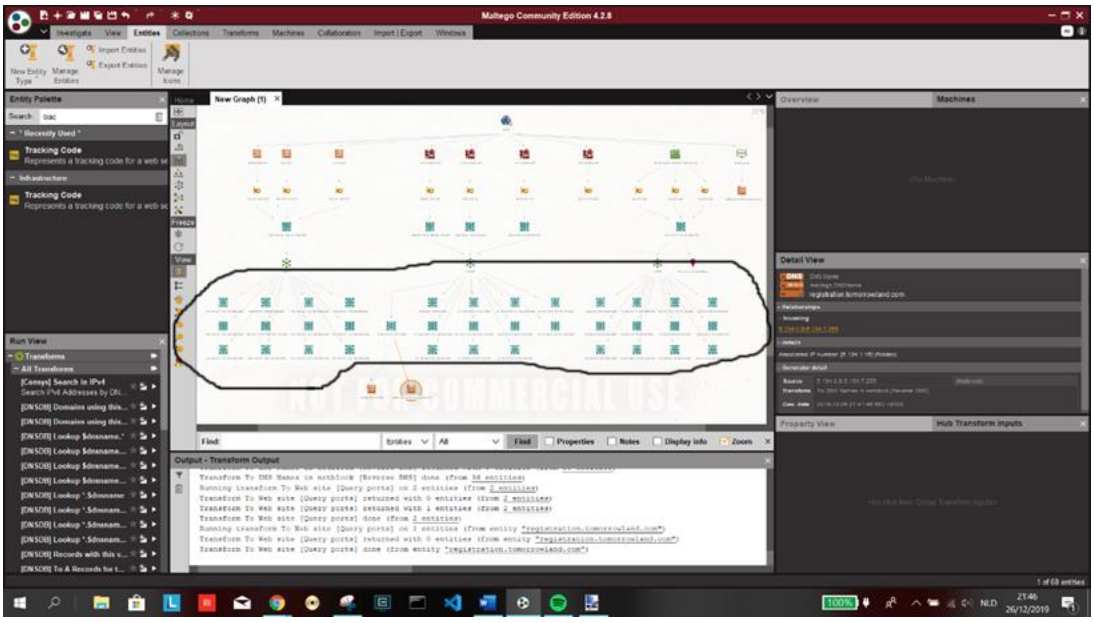
Hierna zoeken we dan naar de AS numbers

AS (Autonomous System): groep IP-netwerken, beheerd door een of meer netwerkoperators met één duidelijk gedefinieerd routeringsbeleid. Bij het uitwisselen van externe routeringsinformatie wordt elk AS geïdentificeerd door een uniek nummer: het Autonomous System Number (ASN). AS = routeringsdomein

zoals te zien is er een server in San Jose, United States.



Nu gaan we van onder naar boven, om te zien of deze organisatie de as nummer bezit of gewoonweg gebruikt, en als er iets wordt gevonden kan je daarna gewoon verder gaan met zoeken naar een dns van de gevonden netblocks, enz..

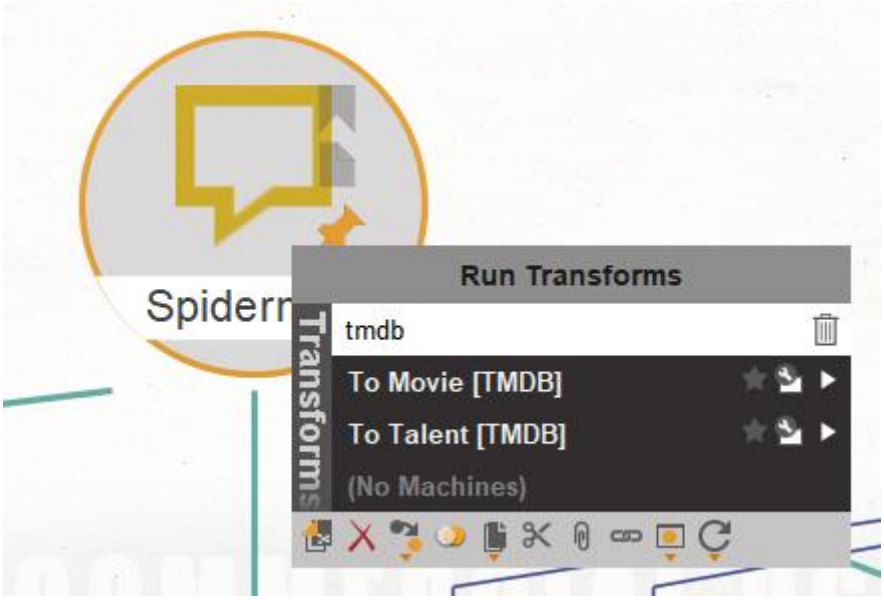


Deze netblocks (omcirkeld) heb ik gevonden toen ik de as nummers heb omgezet naar netblocks om te zien of ze deze bezitten of niet, waardoor ik meerdere netblocks heb gekregen en 1 ervan heb ik dan dns opgevraagd en ik kwam er dan 2 tegen (etools.konvert en registration.tomorrowland.com) en zo kan je eigenlijk hele tijd verder gaan, de keten opnieuw na gaan en volgen.

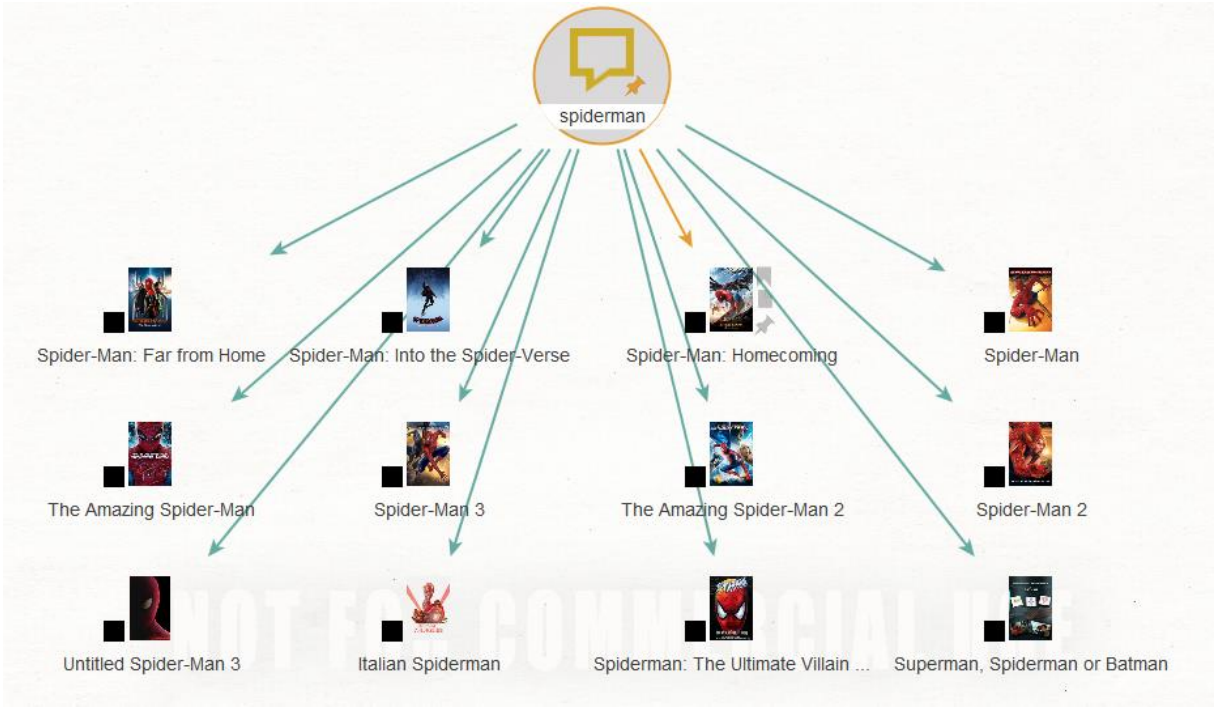
Regular cases

Case 1: *movie database*

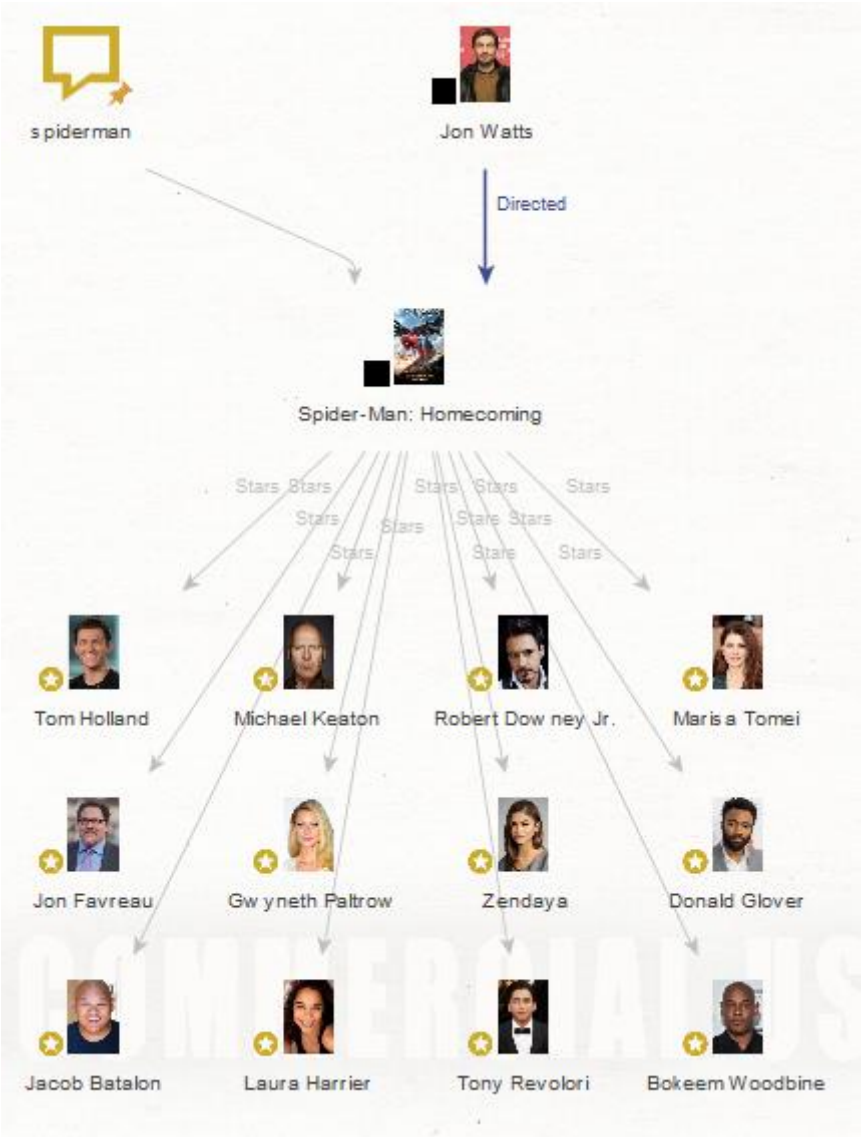
We beginnen eerst met een tekst, hierna heb je de mogelijkheid om de tekst om te zetten naar een film of een talent



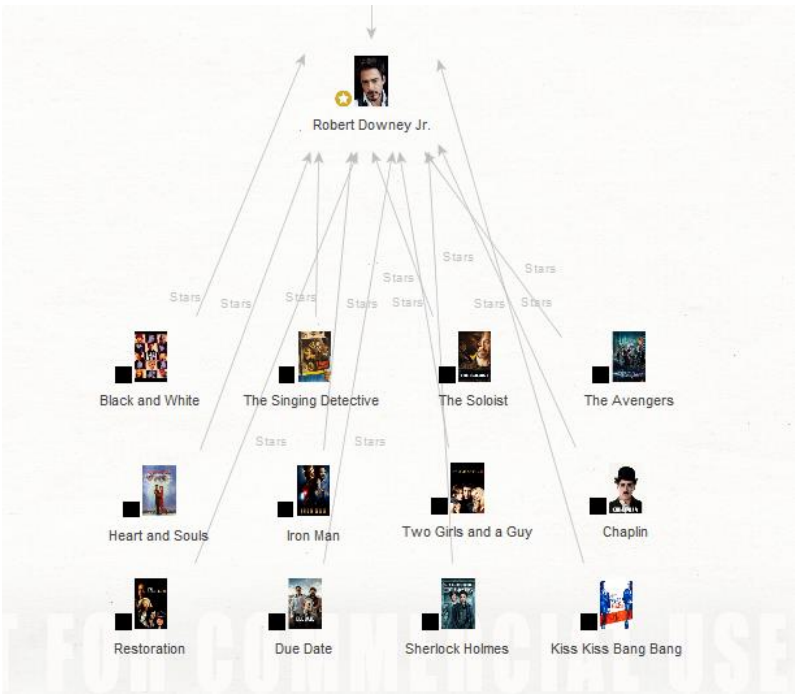
We zetten dus de tekst om naar een film, en we krijgen dan een heleboel films terug, Eens we dit hebben kunnen we vanuit de films ook zien wie de director is en wie er allemaal heeft deelgenomen aan de film, in dit voorbeeld gaan we dan verder met de film Spider-Man: Homecoming

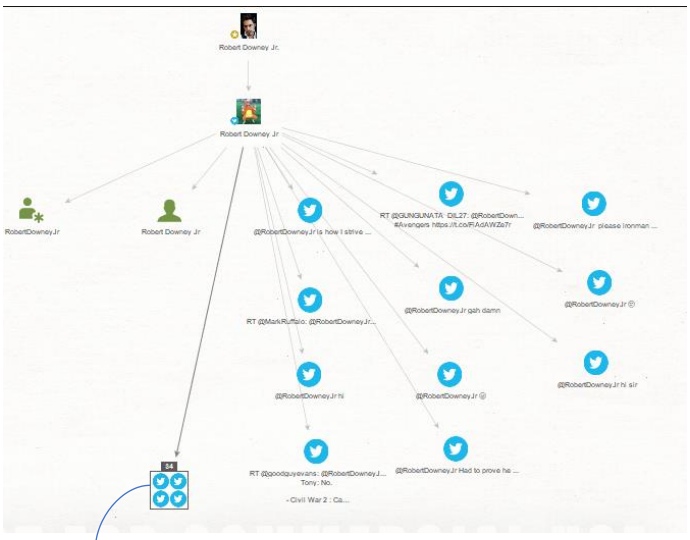


hier zien we dan dan de director en de crew van de film, laten we hier dan verder gaan met Robert Downey Jr.



wat ik van deze persoon wil, is zijn twitter info en in welke andere films hij heeft gespeeld

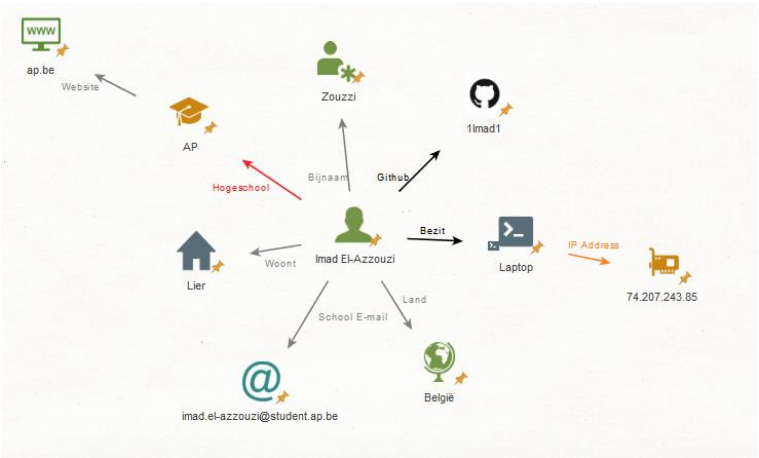




Naar hoeveel personen hij tweets heeft gestuurd, normaal gezien meer maar omdat ik de free versie van Maltego gebruik heb ik een max van 50 entiteiten die ik uithalen

Case 2: *Casefile*

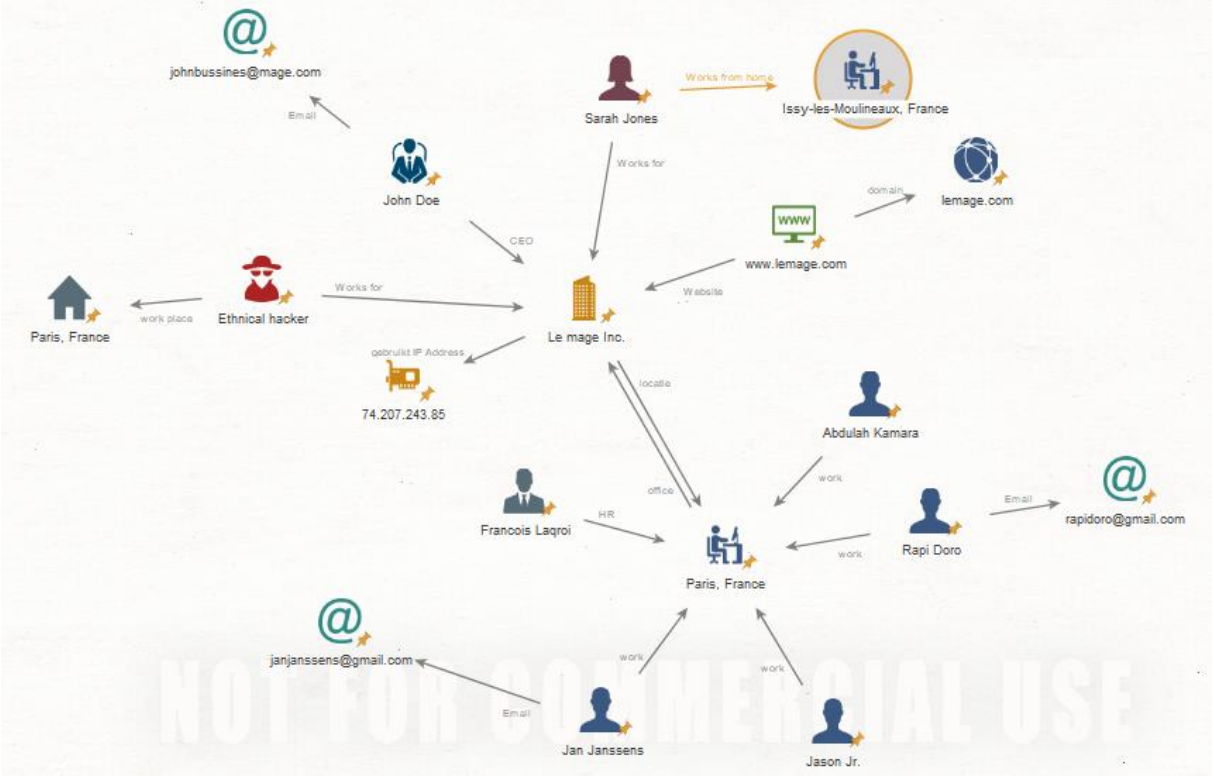
Hier zal ik dan uitleggen wat casefile is, met casefile kan je offline data schetsen in een visuele vorm, casefile is een offline 'analysing' tool, wiens primaire informatiebronnen niet worden verkregen van de open-source intelligentiezijde of programmatisch kunnen worden opgevraagd, dat wilt zeggen dat jij de informatie bepaald (na een analyse) en visueel voorstelt. We zien deze mensen als onderzoekers en analisten die 'op de grond' werken, informatie van andere mensen in het team opdoen en een informatiekaart van hun onderzoek opbouwen. Nou ik zal nu informatie van mezelf en waar ik me plaats vindt analyseren en visueel voort brengen.



Je kan een persoon of een bedrijf analyseren, maar hier heb dan mezelf kort geanalyseerd.

Je kan ook een bepaalde scene analyseren bv een hacker heeft iemand gehackt en hij heeft bepaalde info van de persoon, dan kan hij het doen zoals de afbeelding bovenaan deze tekst.

Ik heb een voorbeeld gemaakt van een fake company in casefile, deze company heeft een CEO, een HR, werknemers, een ethnical hacker voor het bedrijf, een domain, website, IP Address en een paar e-mails. En zo kan je de tool verder gebruiken, security analisten en netwerk engineers van het bedrijf gebruiken casefile voor het checken van kwetsbaarheden van een netwerk



Het duurt wel even voor je echt een bedrijf in casefile in een steekt, maar toevallig na het kijken van een bepaalde filmpje op YouTube waar een persoon een scammer ontmaskert, kwam ik in het filmpje casefile tegen (coincidence? I don't think so)

Als u toevallig nieuwsgierig bent van wat er in het filmpje allemaal gebeurt neem dan zeker een kijkje (https://www.youtube.com/watch?v=RHHzoDqZL8M&t)

Hier zie je dan waarvoor het allemaal kan gebruikt worden, een bedrijf visualiseren na het analyseren van het bedrijf, de mensen en de locatie

Slot

Kort heb ik besproken wat Maltego en Maltego Casefile is, in het begin van het project wist ik niet hoe ik dit moest aanpakken en of dat ik het wel kon doen. Ik begon met het opzoeken van wat de tool is en wat je ermee kan doen, en toen ik Maltego casefile had geïnstalleerd, dacht ik dat ik dat het automatisch was maar ik vergiste me hierin. Ik wou meer dan alleen maar informatie tonen die jezelf in elkaar moet steken, en toen zag ik dat Maltego CE (wat eigenlijk de basis is van de tools die ik gebruikte) het zelfde is maar dit doet het dan automatisch en sneller en dit is het grootte verschil tussen deze tools, maar dit wilt niet zeggen dat casefile saai is of slecht (wat ik daadwerkelijk dacht voor dat ik echt begon) maar toen ik ermee begon te spelen was het een zeer leuke, leerzame en speelse ervaring. Nu ik weet wat Maltego CE is en wat CaseFile is, zal ik deze tools ook in de toekomst gebruiken waar nodig.