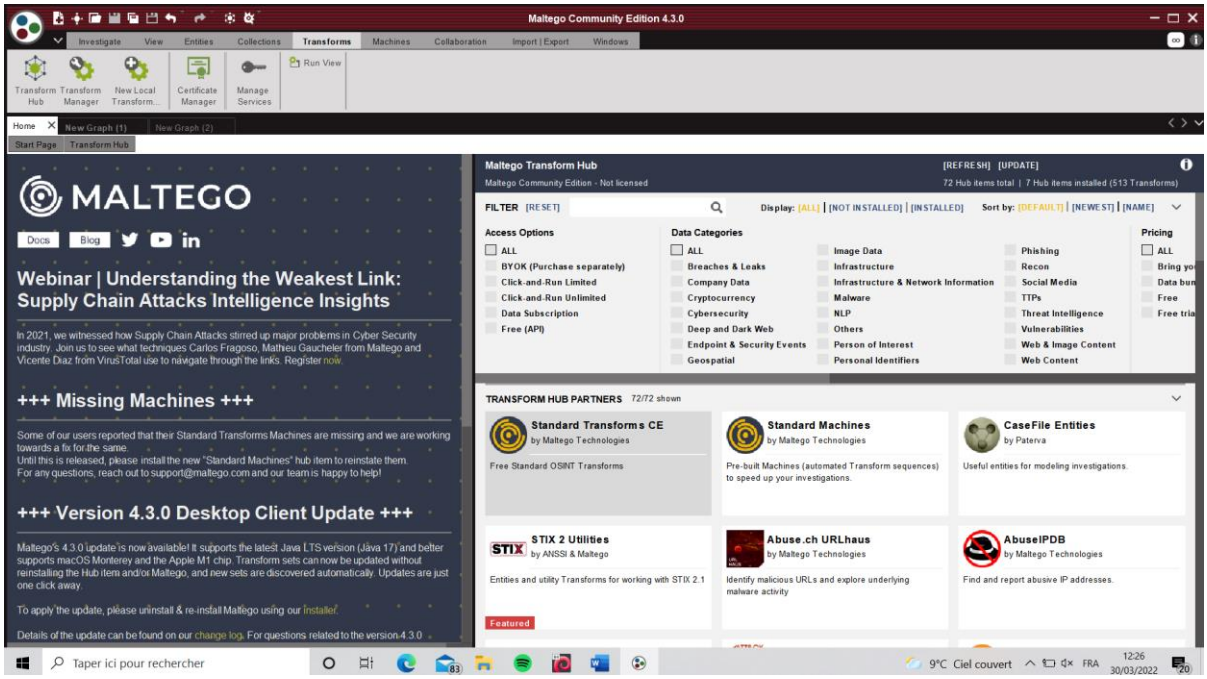
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Département TIC
Filière Télécommunications
Orientation Sécurité de l'information

Laboratoire de SEN

Maltego



Étudiant : **Rosy-Laure Wonjamouna**

Enseignants responsables : **Abraham Rubinstein Scharf**

Stéphane Teixeira Carvalho

Année académique : 2021-2022

Yverdon-les-Bains, le Cliquez ou appuyez ici pour entrer une date.

Table des matières

1 Une simple reconnaissance de réseau

Le nom de domaine que j'ai choisi d'étudier est cara.ch. En effet c'est l'organisation pour laquelle j'ai travaillé en AST. Après avoir exécuté toutes les transformations sur le domaine cara.ch, on obtient le graph ci-après :

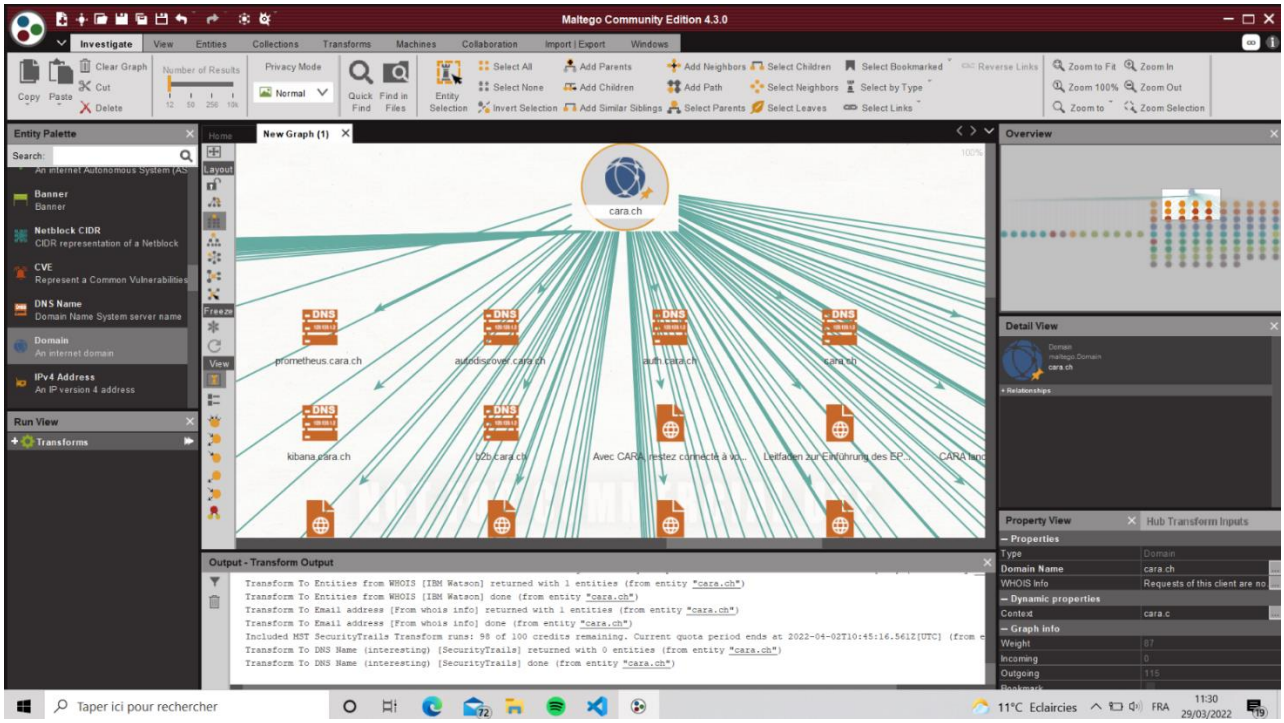


Figure 1: Lancement de all transforms sur le domaine cara.ch

Comme on peut le voir sur cette capture d'écran de nombreux serveurs DNS ont été trouvés.

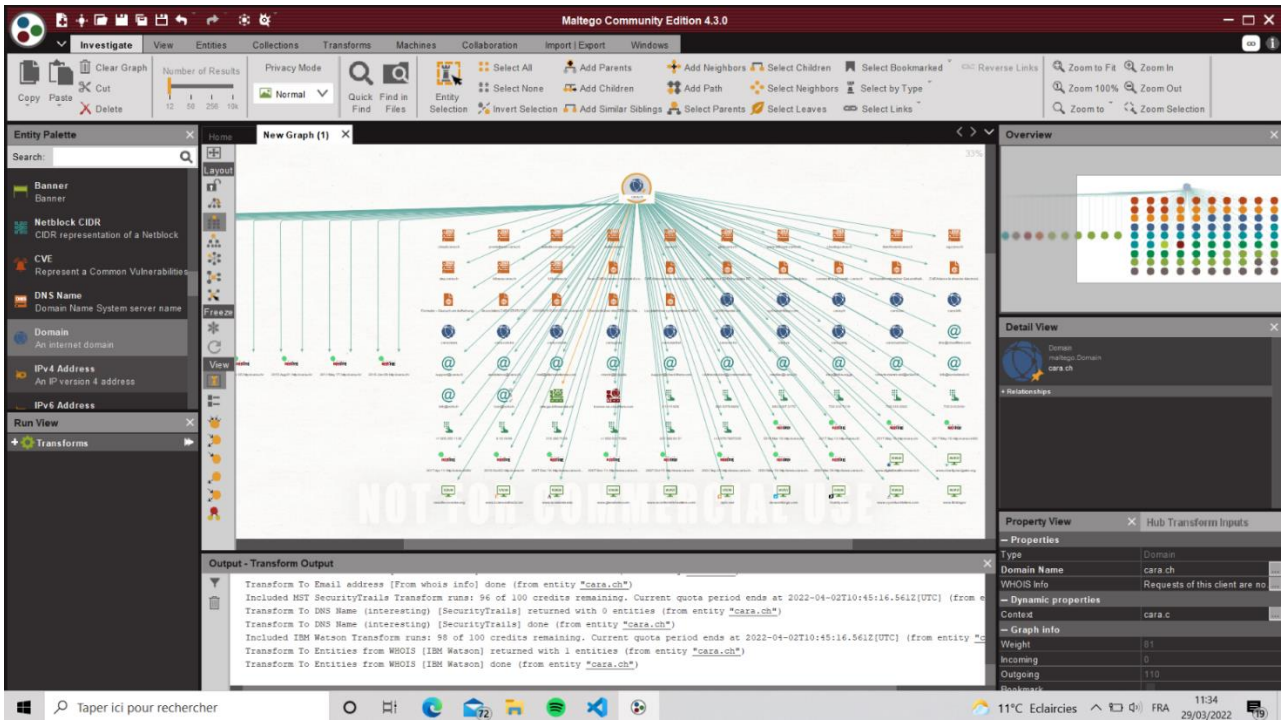


Figure 2: Vue d'ensemble des résultats de "all transforms" sur cara.ch

On a aussi quelques adresses emails liées au domaine cara.ch qui ont été trouvée, ainsi que des serveurs DNS.

Pour la suite du laboratoire j'ai décidé de continuer plutôt avec le domaine epfl.ch car il y a plus de résultats exploitables pour les questions posées après

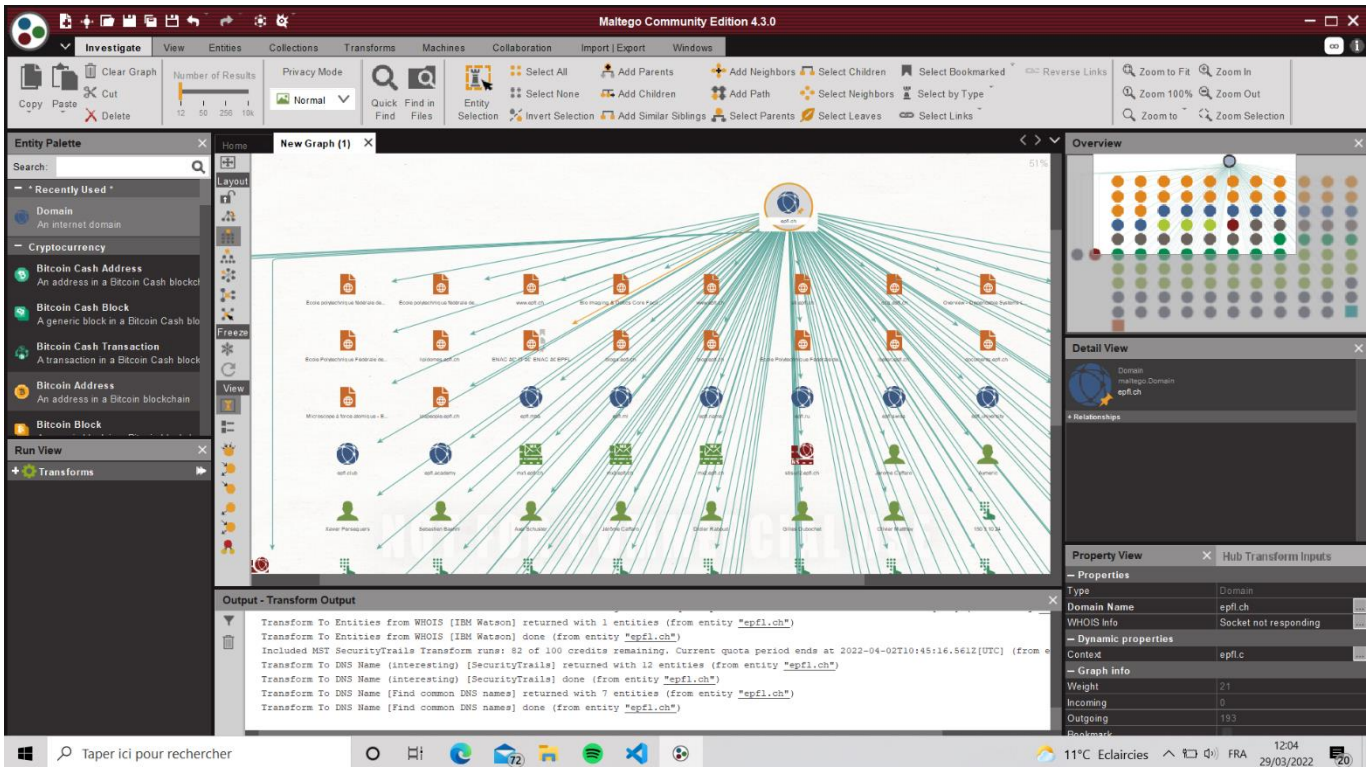


Figure 3: Lancement de "all transforms" sur le domaine epfl.ch

En effet, on obtient des noms de domaines, des sites internet, des personnes, des emails avec ce nom de domaine, des serveurs DNS etc …

Voici quelques autres captures d'écran qui montrent plus en détail ce qui a été trouvé.

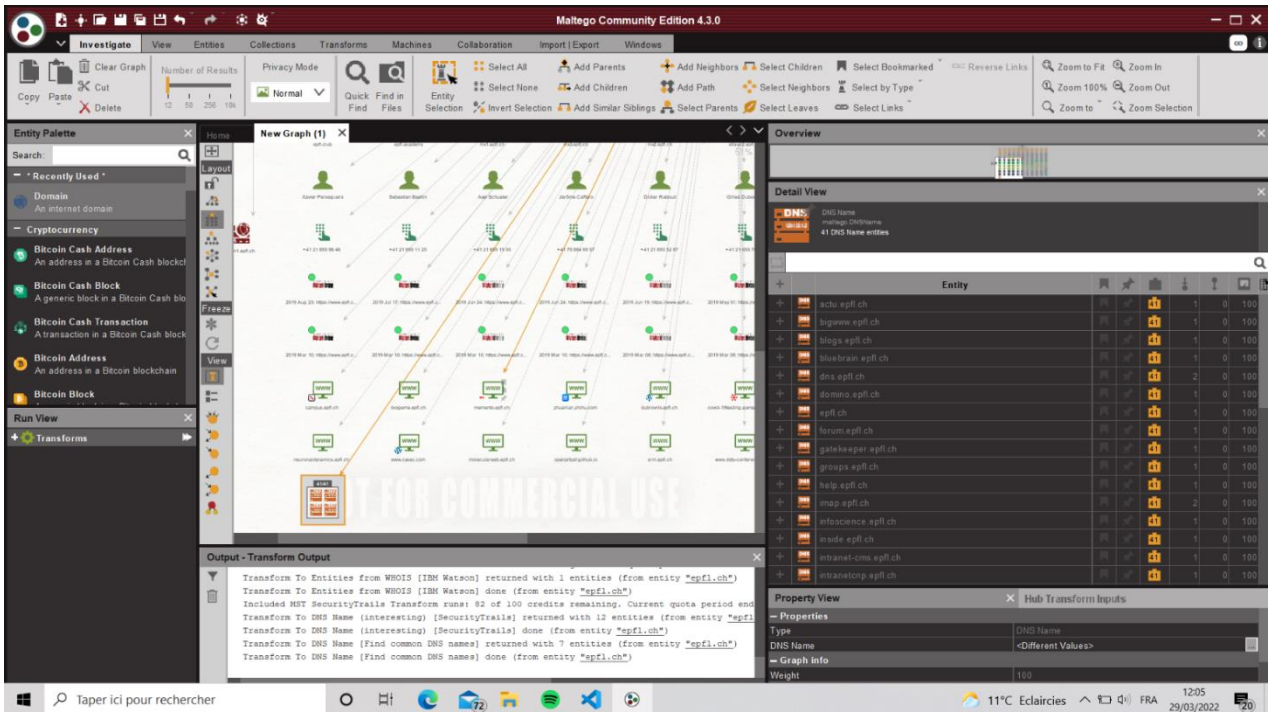


Figure 4: Vue en détails des résultats de "all transforms" sur epfl.ch

On voit ainsi que 41 serveurs DNS différents ont été trouvé, on voit notamment un serveur mail (imap.epfl.ch) et un intranet de l'EPFL.

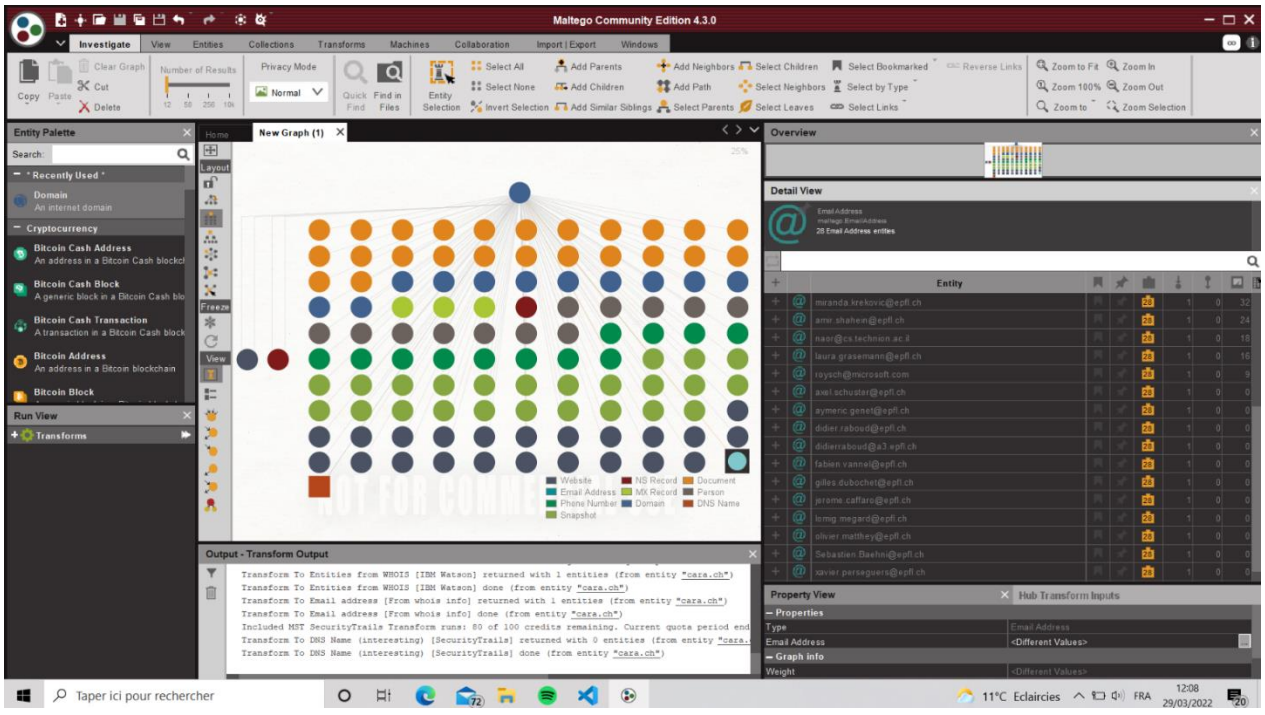


Figure 5: Vue d'ensemble sur les résultats de "all transforms" sur epfl.ch

Ici on peut voir que 29 adresses électroniques liées au domaine EPFL ont été trouvé

On obtient également des numéros de téléphones

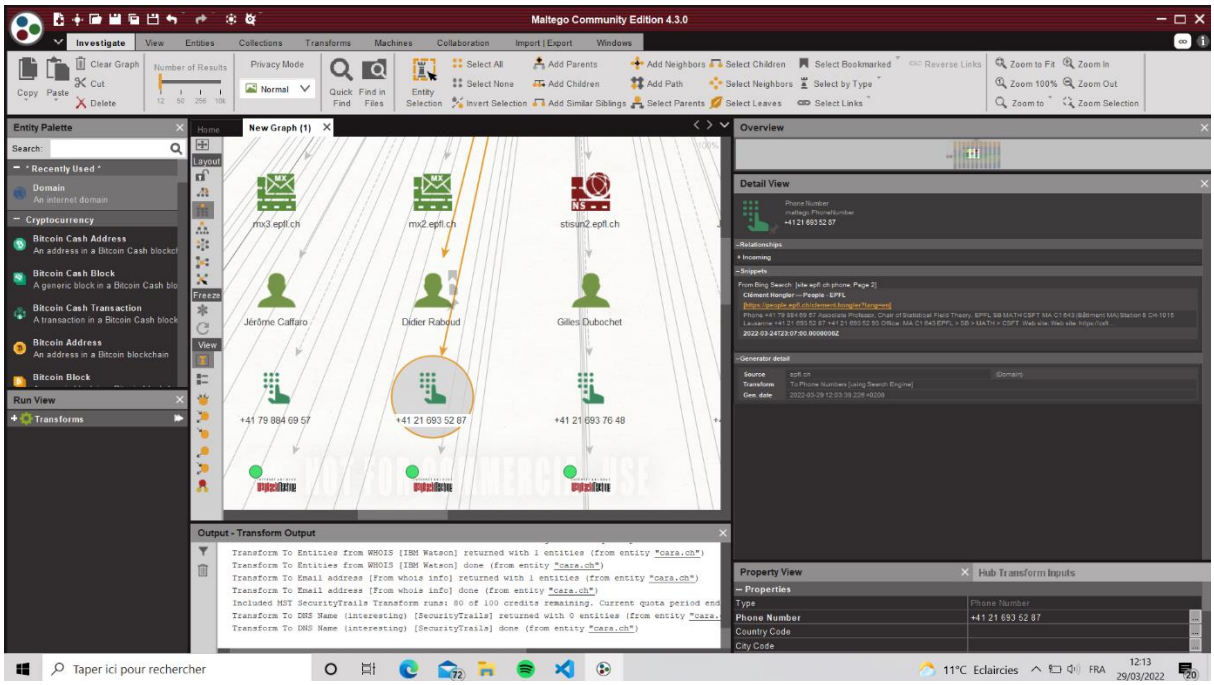


Figure 6: Vue en détails de numéros de téléphone obtenus sur epfl.ch

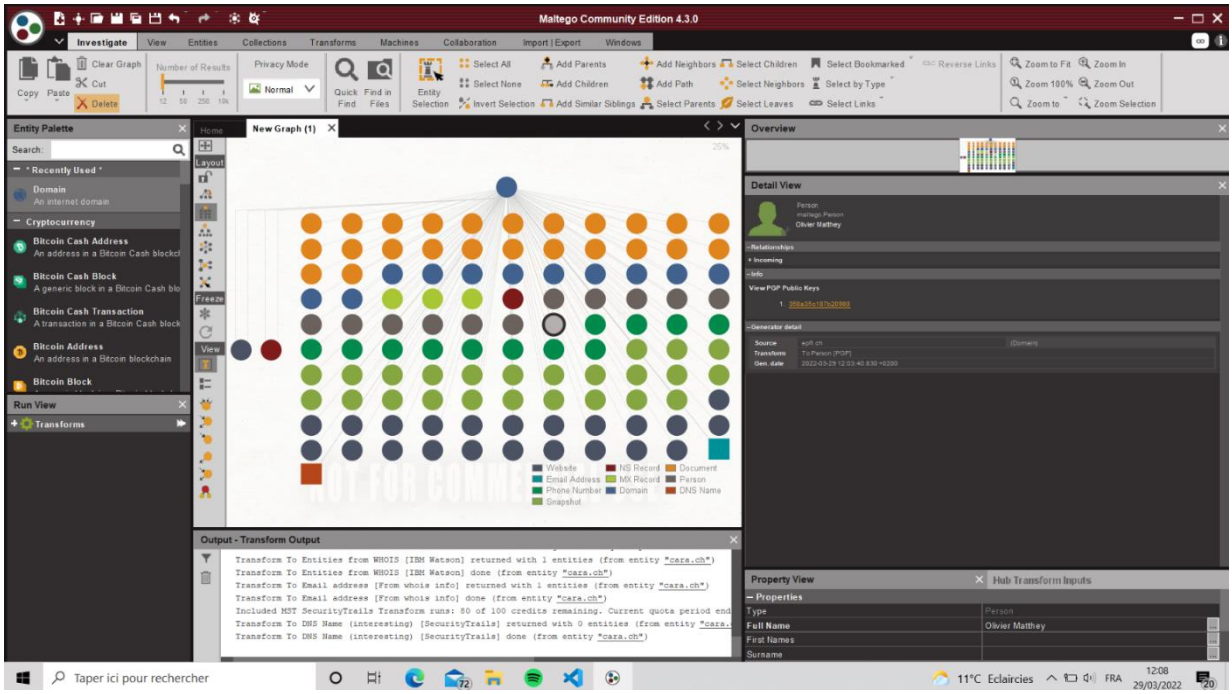


Figure 7: Détail du profil d'une personne liée au domaine epfl.ch

Sur cette capture, on peut voir une des personnes trouvées et sa clé PGP publique associée.

Grâce à cette vue d'ensemble, on peut voir que des sites web, des numéros de téléphones et des documents ont aussi été trouvé !

On va essayer d'investiguer davantage sur la personne d'Olivier Matthey qui a été trouvée

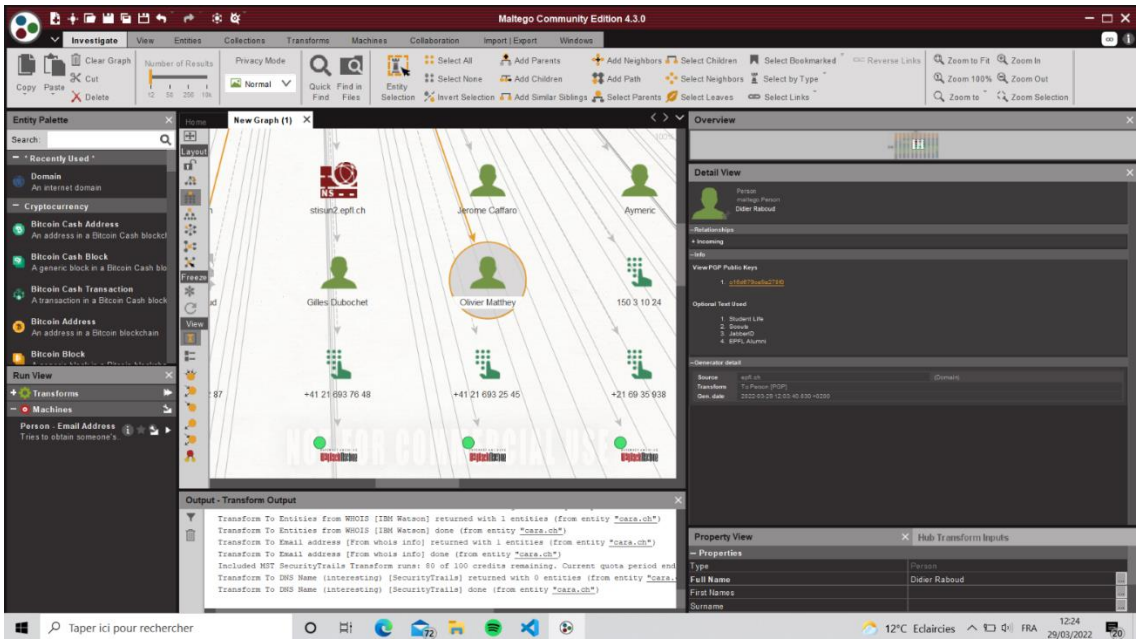


Figure 8: Sélection du profil d'Olivier Matthey

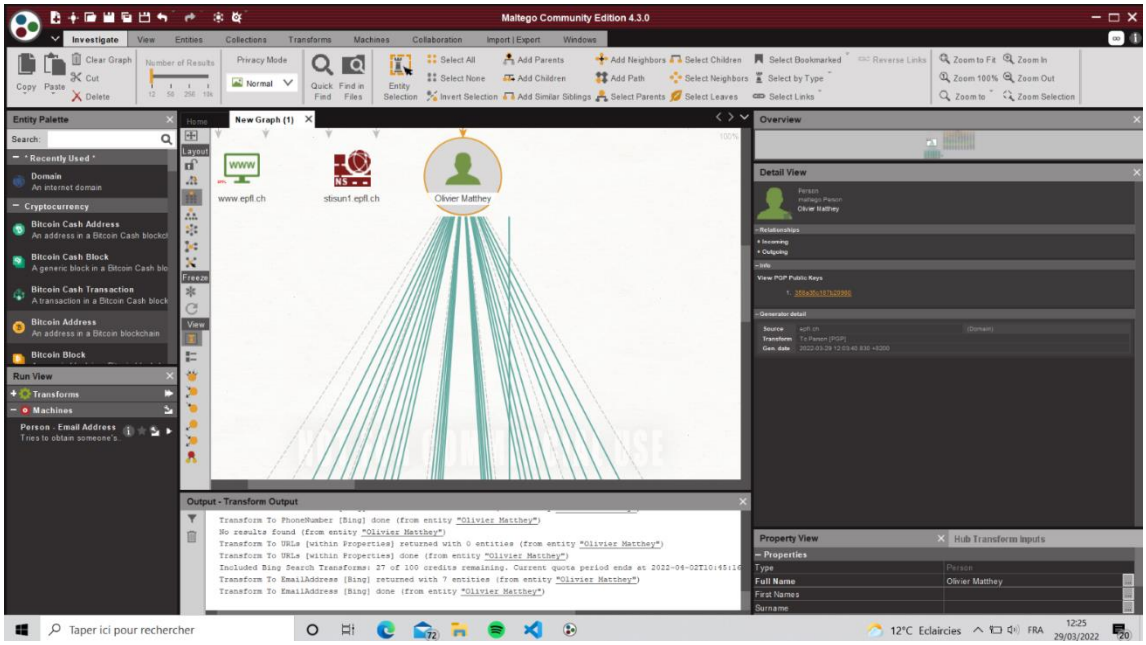


Figure 9: Lancement de "all transforms" sur le profil d'Olivier Matthey

On peut voir ainsi son adresse email EPFL mais aussi d'autres adresses email qu'il est susceptible d'avoir utilisées.

Il semblerait tout de même que certains résultats soient erronés et que ce sont des adresses mails de personnes dont le nom ressemble à celui d'Olivier Matthey qui ont été retrouvées.

2 Recherche d'une identité

J'ai tenté de rechercher quelques identités.

Pour commencer, j'ai cherché ma propre identité. Mais ça s'est avéré infructueux. Il y avait des résultats mais ils étaient tous erronés.

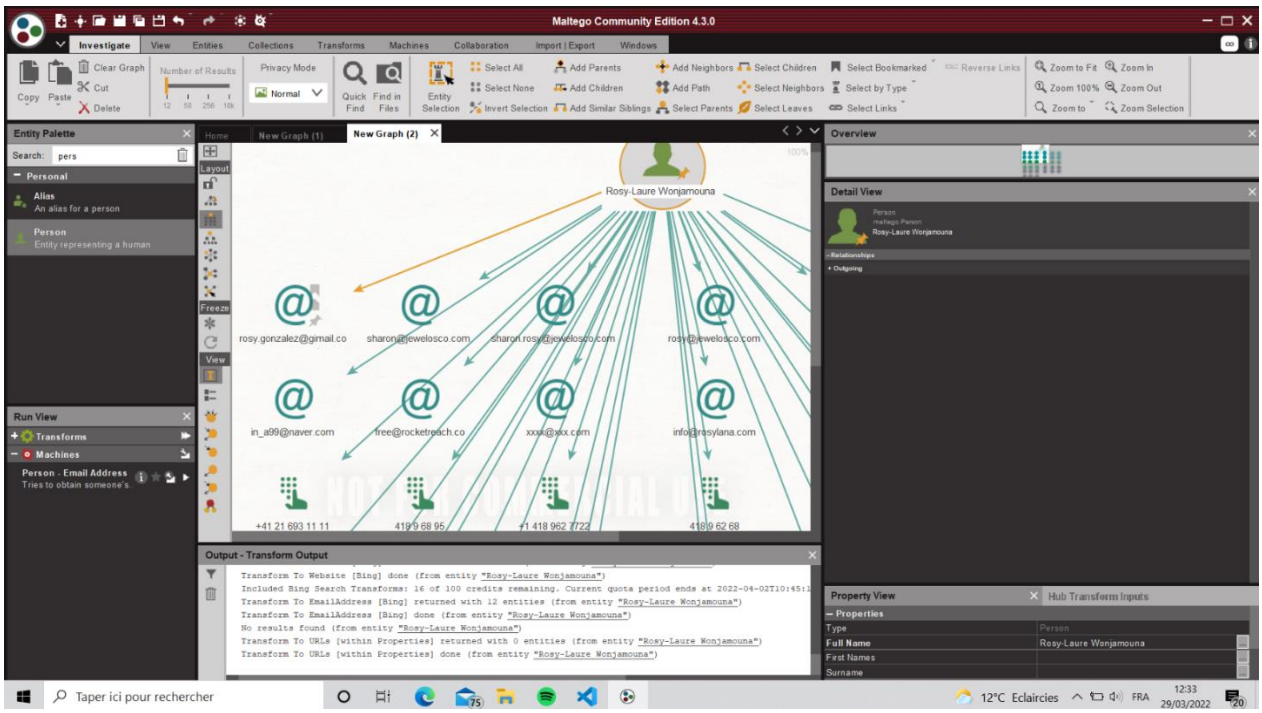


Figure 10: Lancement de "all transforms" sur moi-même

J'ai aussi cherché d'autres personnes que je connais

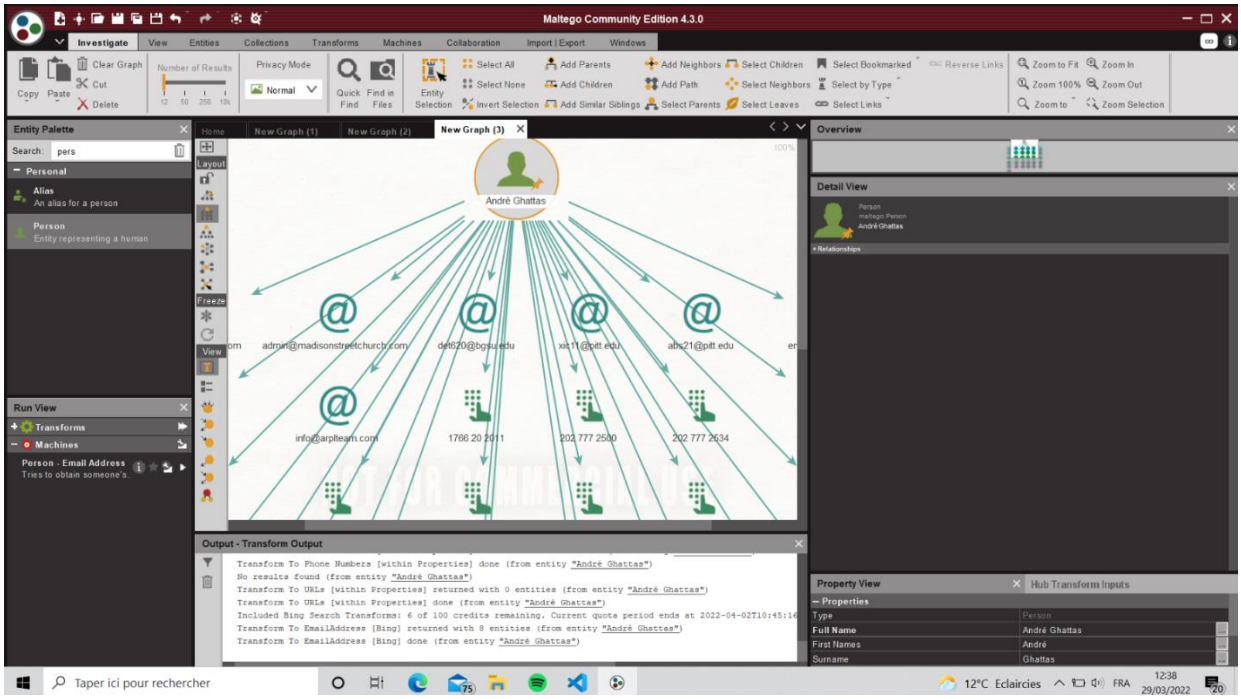


Figure 11: Lancement de "all transforms" sur André Ghattas

André est à l'EPFL mais aucune de ses adresses emails n'a été trouvée ni aucune information véridique.

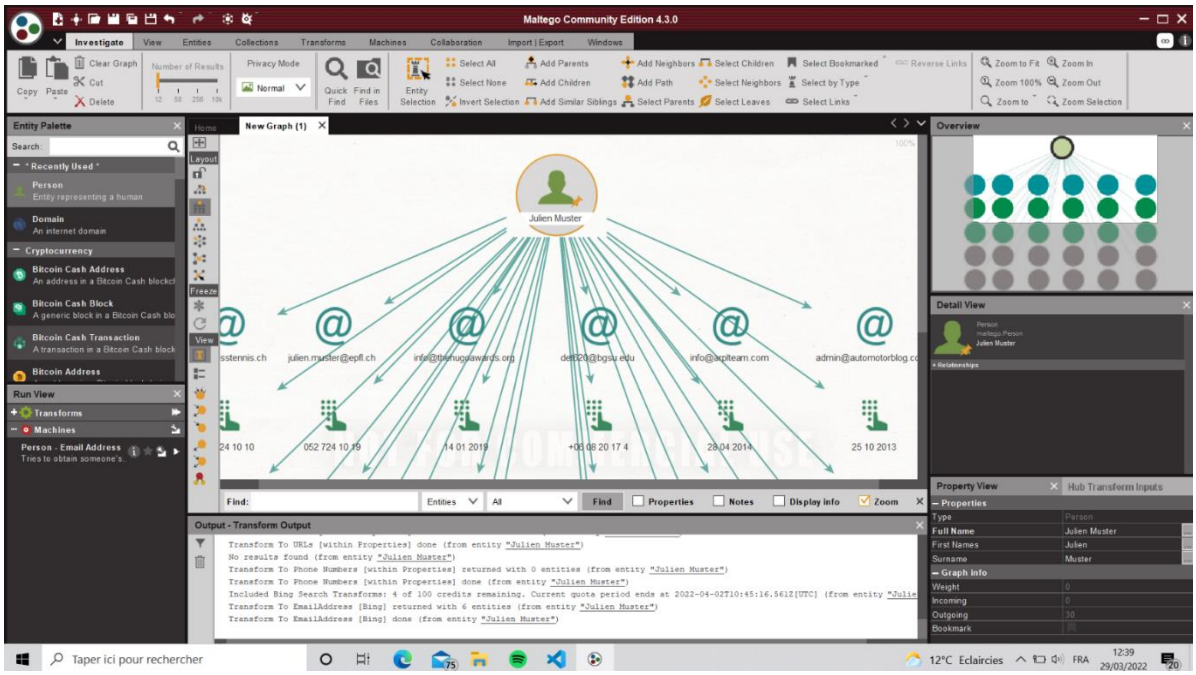


Figure 12: Lancement de "all transforms" sur Julien Muster

Et pour Julien, son adresse email EPFL a été trouvée mais aussi pleins d'autres adresses qui ont l'air erronées

Maintenant on passe aux recherches d'emails.

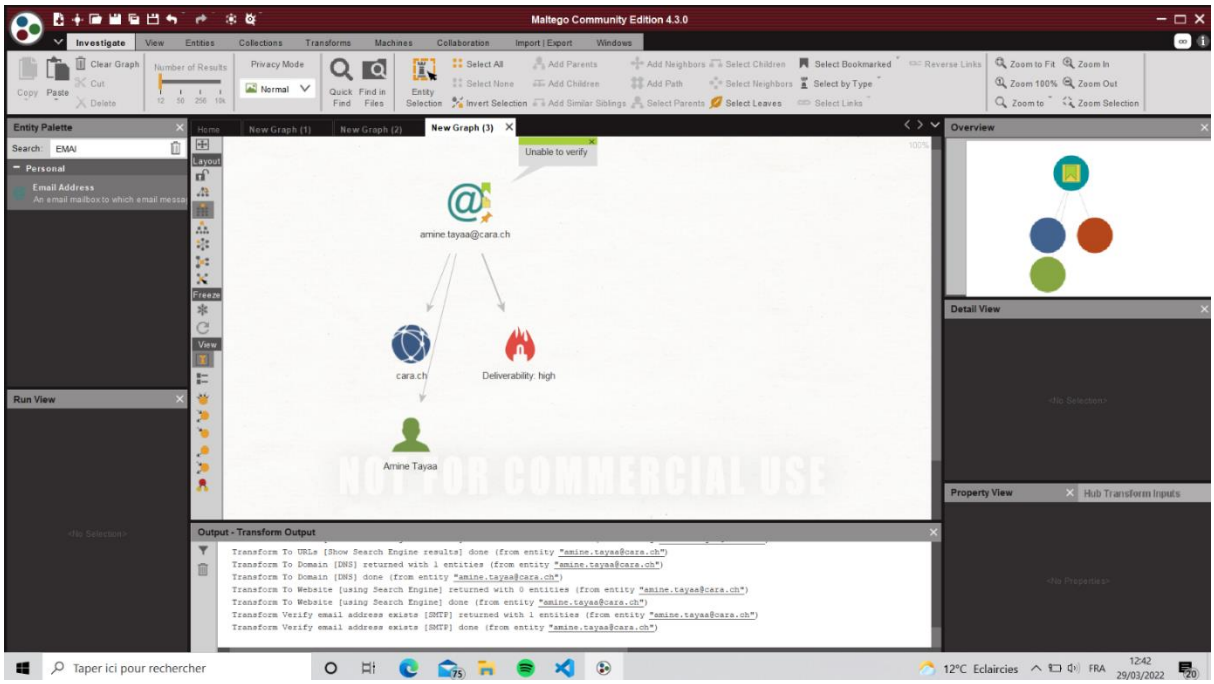


Figure 13: Lancement de "all transforms" sur le mail d'Amine Tayaa

J'ai cherché la personne de contact que j'avais chez CARA. Des liens avec CARA ont été trouvé. Mais rien de non évident. Maltego indique aussi qu'il n'arrive pas à vérifier l'email d'Amine

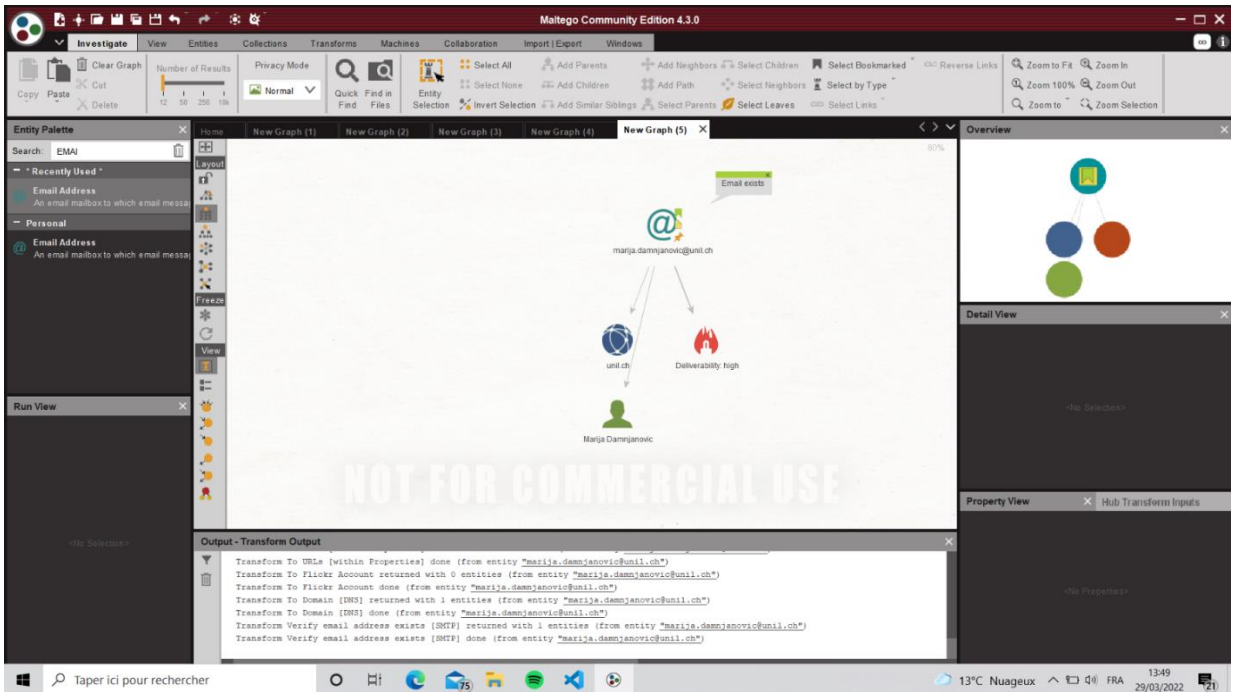


Figure 14: Lancement de "all transforms sur le mail de Marija Damnjanovic

Ici on peut voir que l'email de Marija est vérifié comme étant existant par Maltego mais aucun lien non évident n'a été trouvé

3 Installation et utilisation de nouvelles transformations

J'ai décidé d'utiliser les nouvelles transformations sur le domaine cara.ch pour pouvoir y trouver plus d'informations.

Maintenant on execute la transformation VirusTotal

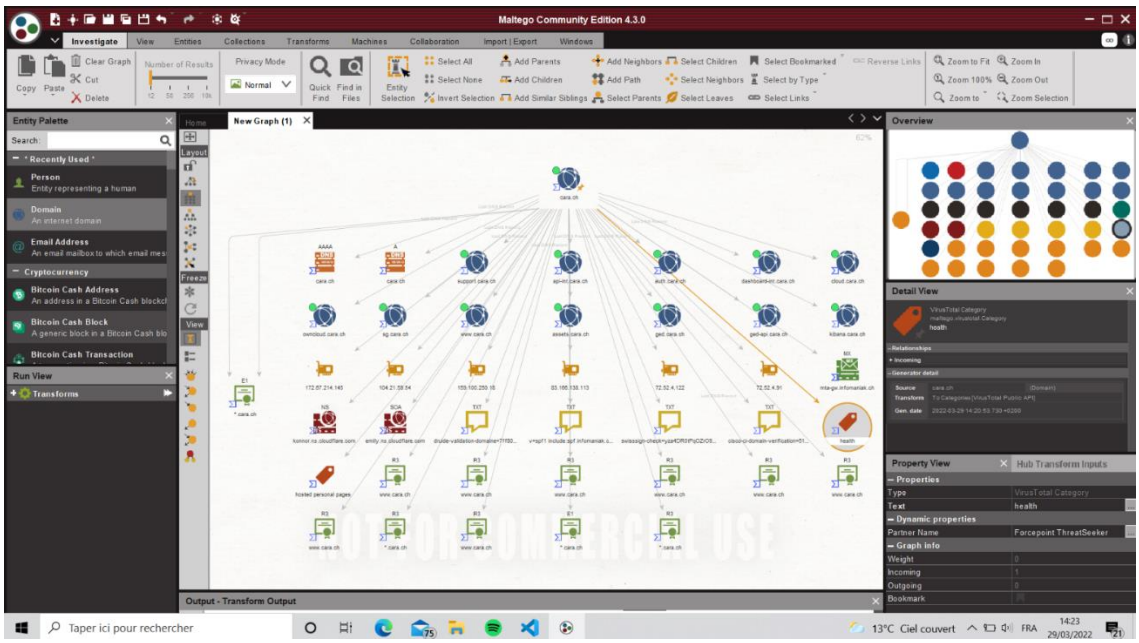


Figure 15: Lancement de la transform "Virus Total" sur cara.ch

On voit que plus de noms de domaines qui n'avaient pas été trouvé précédemment. Par exemple les domaines support.cara.ch, api-int.cara.ch et dashboard-int.cara.ch n'ont pas été trouvé.

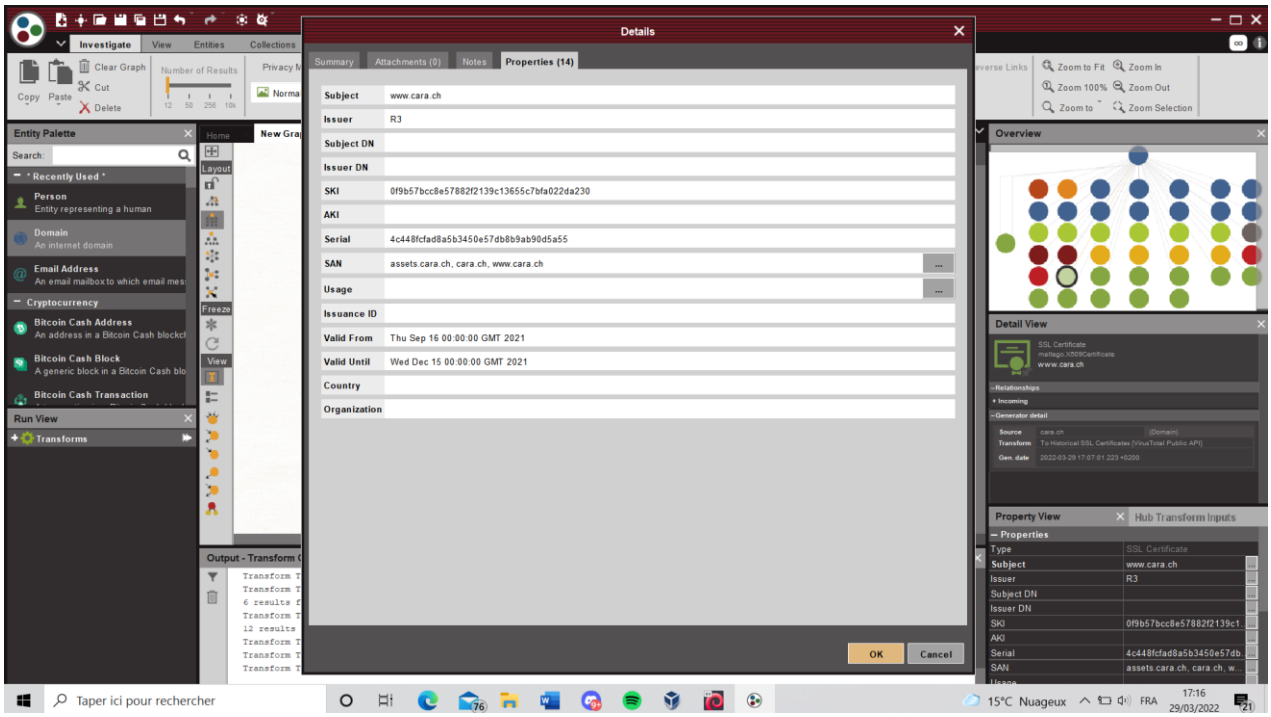


Figure 16: Détail du certificat SSL trouvé par la transform "Virus Total"

Il y a aussi des certificats SSL pour www.cara.ch qui ont été trouvé.

Ici on execute PassiveTotal

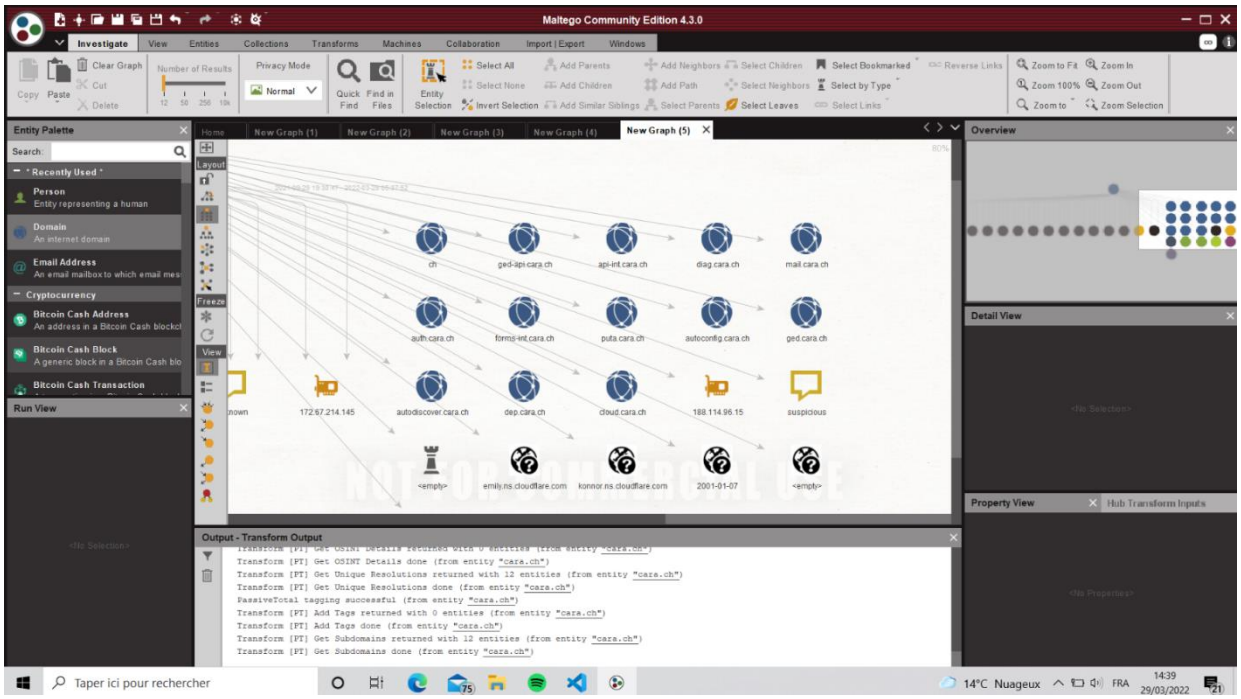


Figure 17: Lancement de la transform "Passive Total" sur le domaine cara.ch

mail.cara.ch est un nouveau domaine qui a été découvert. Des adresses IP associées au domaines ont aussi été découvertes en plus

Après l'exécution de shodan on obtient :

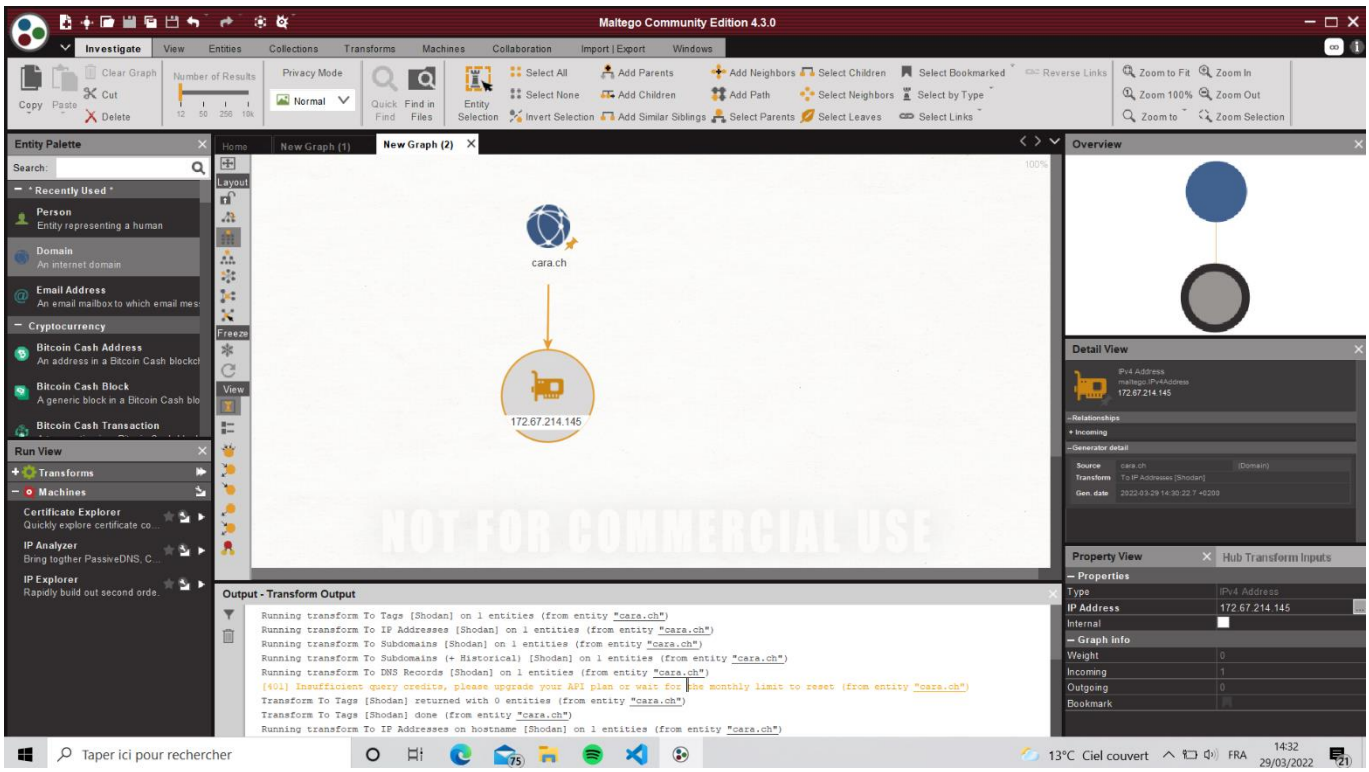


Figure 18: Lancement de la transformation "shodan" sur cara.ch

J'ai essayé d'executer cette transformation sur le domaine epfl.ch mais je n'ai rien obtenu de plus qu'une adresse IP. En voyant que le résultat était le même pour les deux domaines, je me suis demandé à quel résultat j'arriverai en lançant VirusTotal et PassiveTotal sur le domaine epfl.ch.

Voici les captures d'écran des résultats :

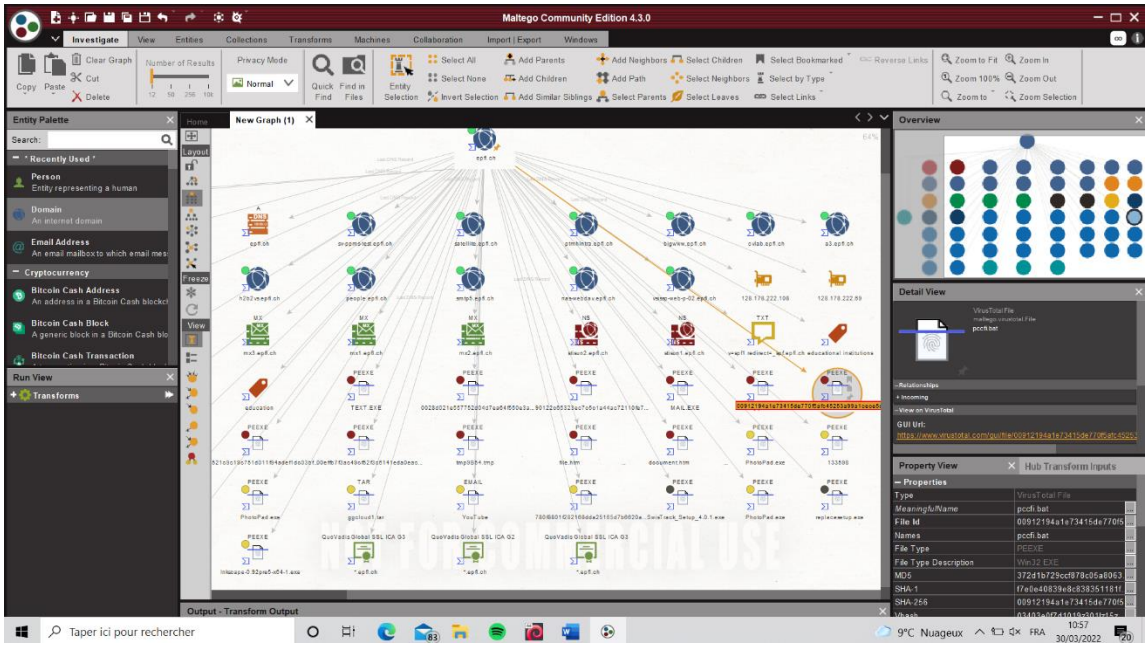


Figure 19: Lancement de la tranform "VirusTotal" sur epfl.ch

On obtient des hashes de malwares, des noms de fichiers suspects etc …

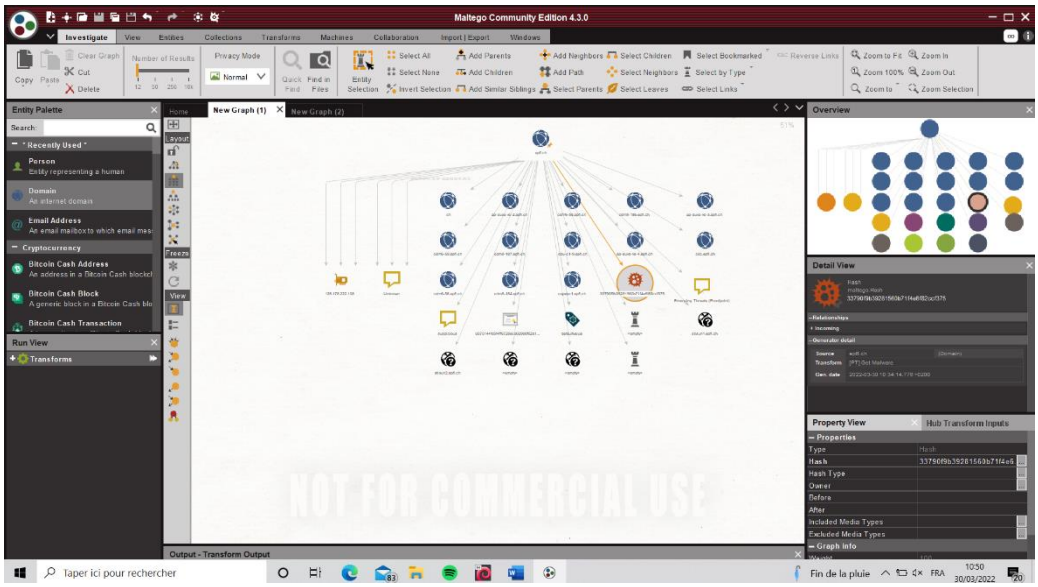


Figure 20: Lancement de la transform "PassiveTotal" sur epfl.ch

Ici aussi, on obtient un malware hash sur le domaine epfl.ch en plus des noms de domaines liés

Faisons un petit tableau récapitulatif des transformations installées :

Virus Total (Public API)	Passive Total	Shodan
C'est quoi ? **Permet d'analyser des fichiers et des URLs pour chercher des malwares.**	C'est quoi ? Plateforme de recherche de menaces. Elle permet d'analyser la sécurité des systèmes avant que les attaques n'arrivent.	C'est quoi ? Analyseur d'internet : donne des informations intéressantes (aussi en sécurité) sur des dispositifs connectés, des serveurs et des services ;
Résultats obtenus sur cara.ch **De nouveaux noms de domaines liés** **Des certificats SSL**	Résultats obtenus sur cara.ch De nouveaux noms de domaines Rien de plus de significatif	Résultats obtenus sur cara.ch Une adresse IPv4
Résultats obtenus sur epfl.ch **Des fichiers suspects** **Des malware hashes** **De nouveaux noms de domaines liés**	Résultats obtenus sur epfl.ch De nouveaux noms de domaines liés Un malware hash Un certificat SSL	Résultats obtenus sur epfl.ch Une adresse IPv4

4 Installation et utilisation de nouvelles transformations

Ils restent quelques transforms gratuites et intéressantes que l'on pourrait installer. Je vais utiliser trois d'entre elles que sont Have I Been Pwned, Farsight DNSB, et FullContact. J'ai voulu utiliser dataprovider aussi mais je n'ai pas pu l'installer sur Maltego. J'en ai tout de même fait mention dans mon tableau récapitulatif. J'ai fait le choix de les lancer sur le domaine epfl.ch

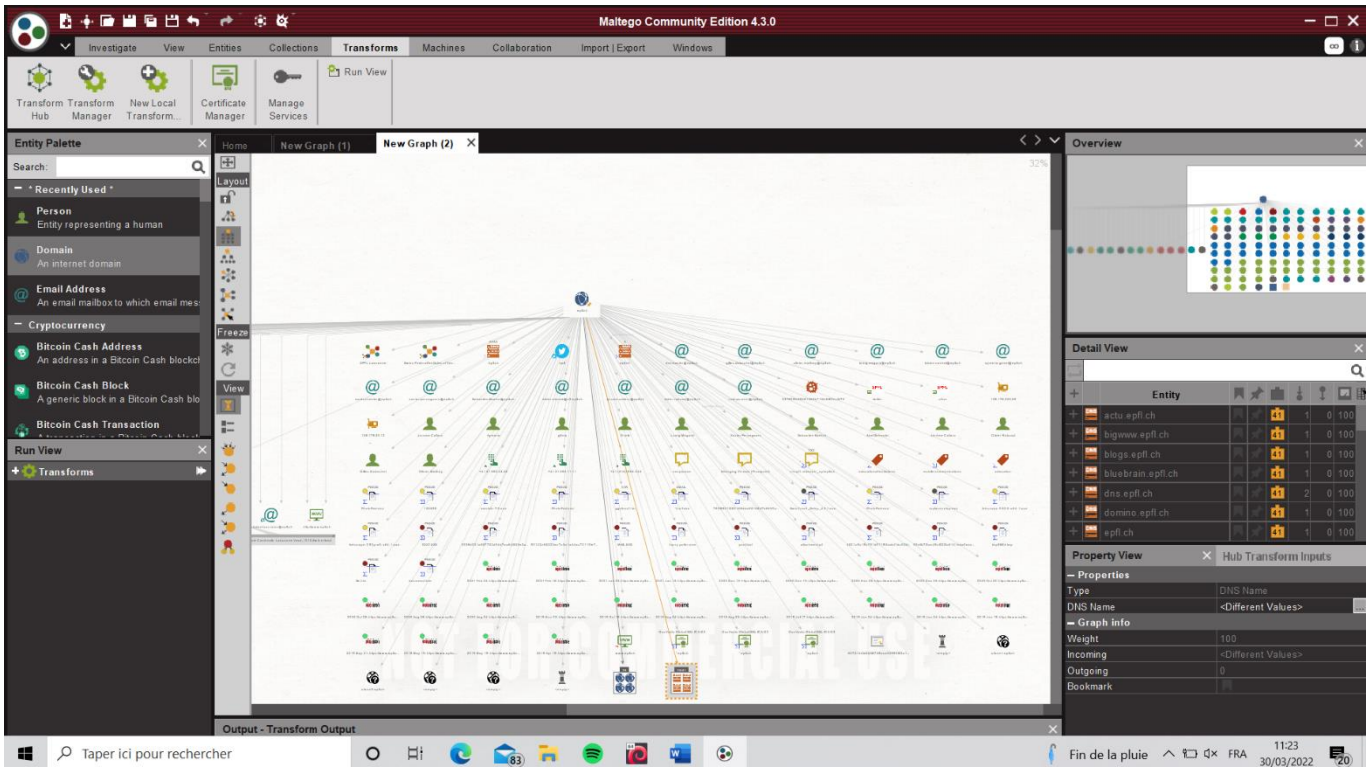


Figure 21: Lancement de "all transforms" avec les dernières transforms installées sur epfl.ch

On peut constater que par rapport au lancement précédent de la commande all transforms sur le domaine epfl.ch le graph construit contient bien plus de détails. Ici on peut voir que les noms de domaines trouvés et les serveurs DNS trouvés ont été regroupés dans une seule icone pour faciliter la lecture du graph qui contient maintenant bien d'autres détails générés par les autres transforms.

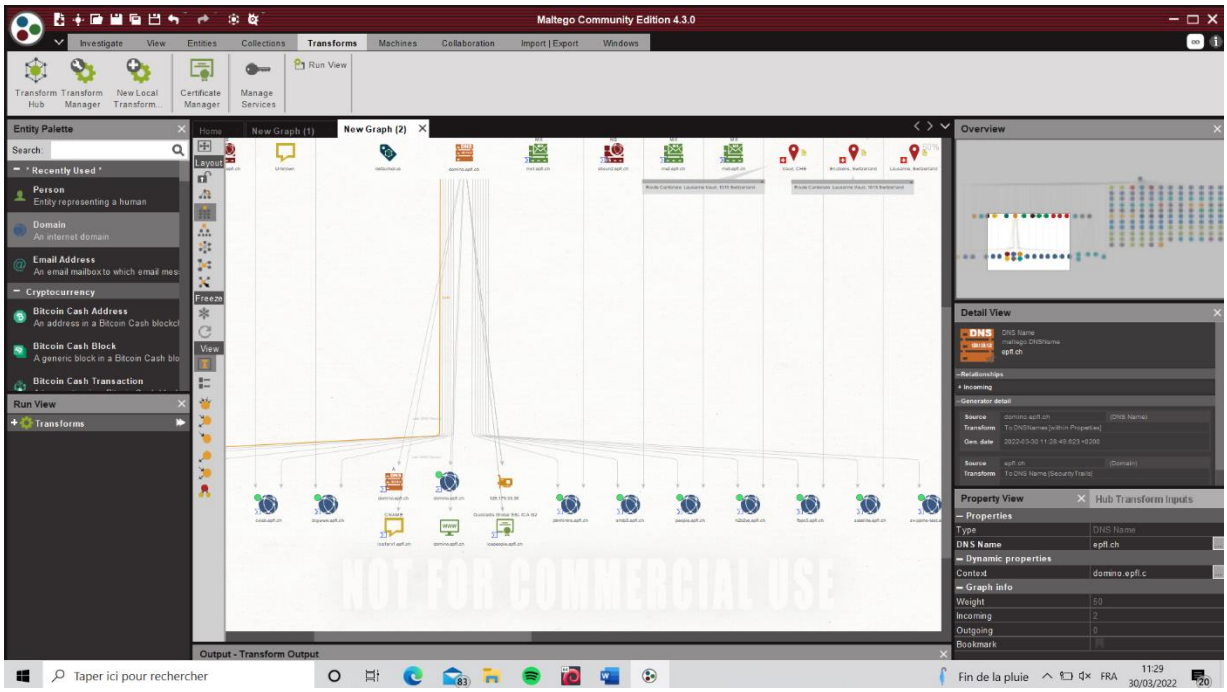


Figure 22: Lancement de Farsight DNS sur un des serveurs DNS du domaine epfl.ch

En lançant Farsight sur le serveur DNS on obtient d'autres détails, d'autres noms de domaines exploitables avec une adresse IP. Le graph devient de plus en plus difficile à naviguer mais on obtient des résultats qui pourraient être exploitable dans le cadre d'une attaque.

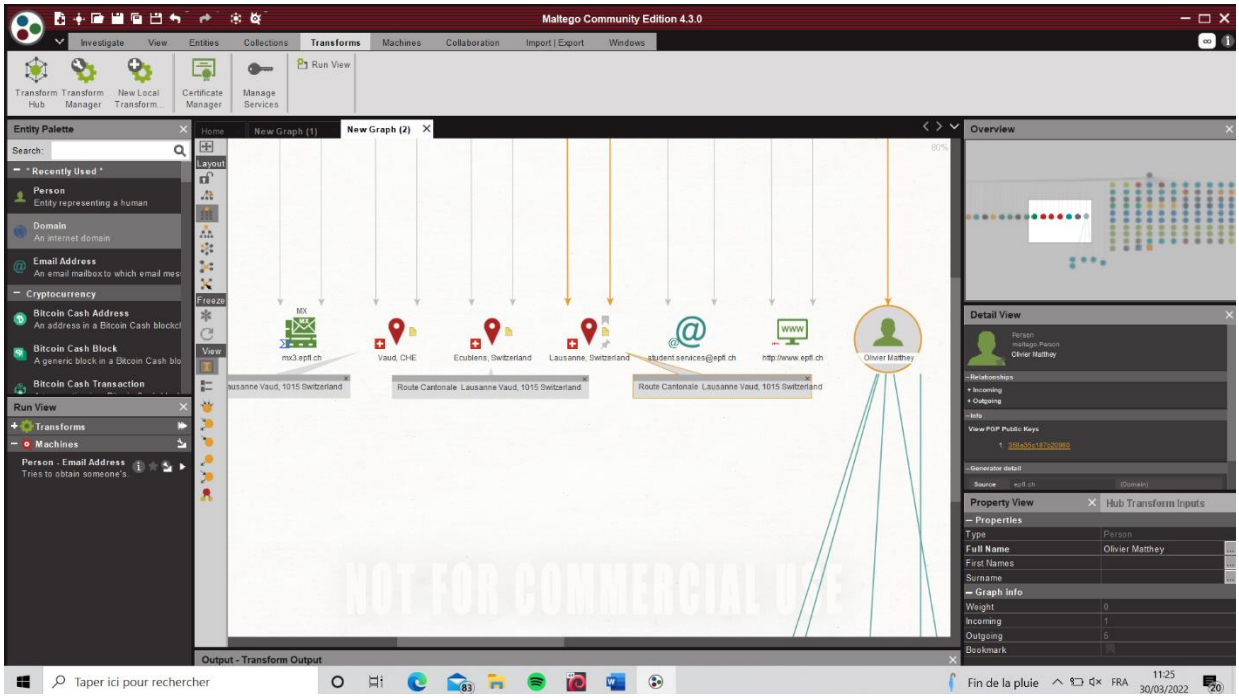


Figure 23: Vue en détail des adresses trouvées

Ici on peut voir l'apport de la transform FullContact sur le graph. En effet, on a maintenant l'adresse de l'EPFL qui est affichée dans le graph. On peut vérifier qu'il s'agit bien là de l'adresse de l'EPFL. On remarque aussi figure 21, qu'un compte twitter associé au domaine a également été trouvé.

J'ai lancé Have I been Pwned sur une des adresses emails de l'epfl :

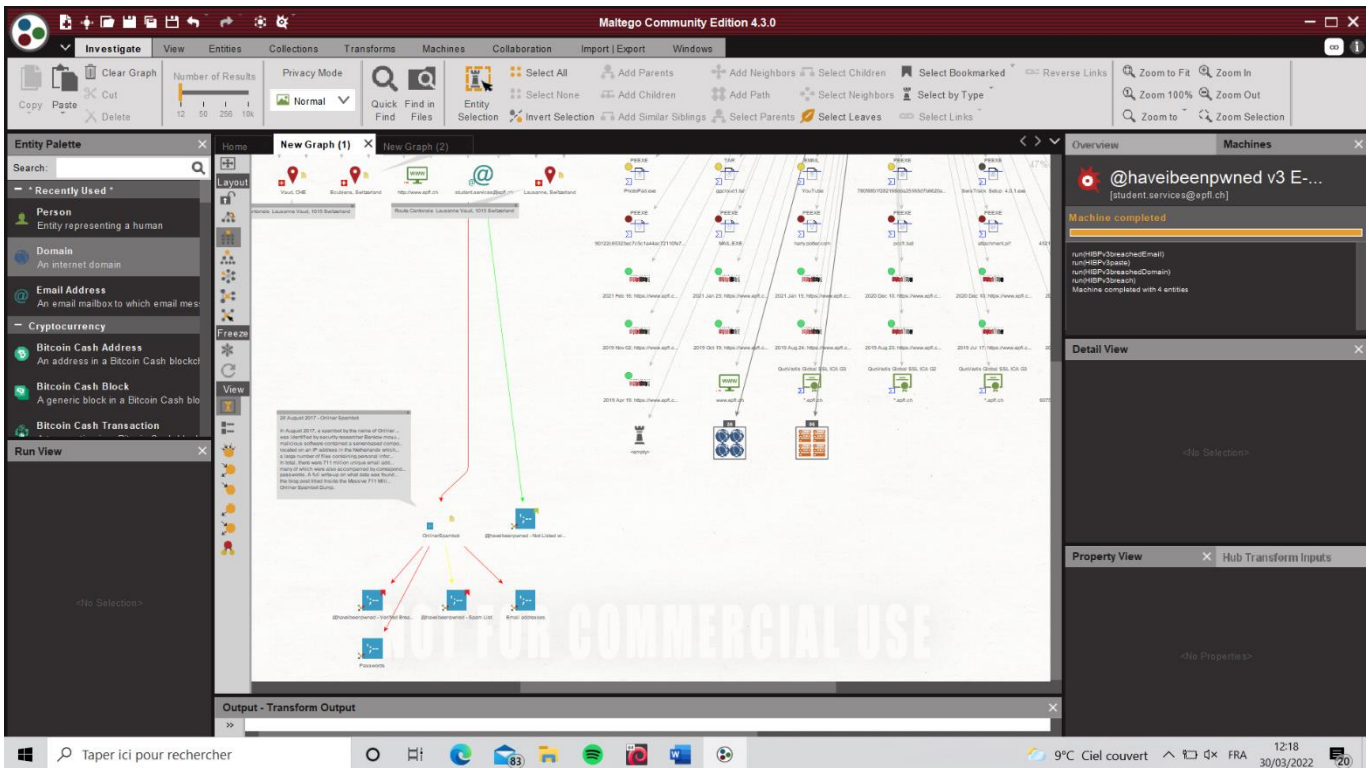


Figure 24: Lancement de la transform "Have I been Pwned?" sur l'email student.services@epfl.ch

On peut déduire de l'embranchement créé dans le graph par la transform que cet email aurait été victime d'une éventuelle compromission d'un bot (Onliner SpamBot) ayant conduit au leak d'un mot de passe utilisé pour cette boîte mail en août 2017.

Faisons un petit tableau récapitulatif des transformations installées :

Have I Been Pwned	Dataprovider	Farsight DNSDB	FullContact
C'est quoi ? **Permet de vérifier si une éventuelle compromission de données a eu lieu, si des mots de passe ont leaké.**	C'est quoi ? Une des plus grandes bases de données au monde contenant des données de sites web publics. Elle contient plus de 280 millions de domaines. On peut utiliser les données contenues pour découvrir de nouveaux chemins dans le réseau, plus de liens, d'adresses IP, d'e-mail etc …	C'est quoi ? La plus grande base de données liée au DNS du monde Facilite l'exposition de tous les domaines liés à un DNS (ainsi que NX, MX, AAAA, SOA etc …)	C'est quoi ? Connecte des fragments de données d'un individu afin d'avoir un profil complet sur cette personne soit des noms, des adresses postales, des emails, des numéros de téléphones, des comptes Twitter etc …