

# Maltego

# SEN

---



Eric Bousbaa

30 mars 2022

## Reconnaissance du réseau heig-vd.ch

La recherche s'effectue sur le domaine heig-vd.ch.

Concernant les dates demandées avant de lancer la transformation - qui doivent probablement correspondre aux recherches effectuées sur [wayback machine](#), nous utilisons les paramètres suivants :

- Begin date : 1er janvier 2010 (2010 01 01, format YYYY MM DD)
- End date : 3 mars 2022 (2022 03 03, format YYYY MM DD), qui est la date du début de ce laboratoire.

Ceci devrait couvrir une durée suffisamment longue pour être analysée.

En lançant la commande **run all transform**, Maltego trouve les éléments suivants :

- des documents - trouvés sur internet

 maltego.Document	EINEV – HEIG-VD
 maltego.Document	Journal de travail – HEIG-VD
 maltego.Document	Fiche de cours – webwww03 – poseidon.heig-vd.ch
 maltego.Document	HEIG-VD
 maltego.Document	webwww03 – poseidon.heig-vd.ch
 maltego.Document	DESIGN AND LOCOMOTION CONTROL FOR A TELEROBOT – HEIG-VD
 maltego.Document	php.iai.heig-vd.ch
 maltego.Document	cfb.heig-vd.ch
 maltego.Document	和文タイトル – files.iai.heig-vd.ch
 maltego.Document	Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud ...
 maltego.Document	sv-lncs – HEIG-VD
 maltego.Document	heig-vd.ch
 maltego.Document	mistic.heig-vd.ch
 maltego.Document	HEIG-VD
 maltego.Document	Éric Taillard

- Des noms DNS - des noms de serveurs DNS

DNS	maltego.DNSName	wodfusion.heig-vd.ch
DNS	maltego.DNSName	gaps-prov.heig-vd.ch
DNS	maltego.DNSName	oe18.heig-vd.ch
DNS	maltego.DNSName	mistic.heig-vd.ch
DNS	maltego.DNSName	iai.heig-vd.ch
DNS	maltego.DNSName	reds-data.heig-vd.ch
DNS	maltego.DNSName	heig-vd.ch
DNS	maltego.DNSName	smapshot.heig-vd.ch
DNS	maltego.DNSName	glpi085.heig-vd.ch
DNS	maltego.DNSName	go.heig-vd.ch
DNS	maltego.DNSName	planid.heig-vd.ch
DNS	maltego.DNSName	imap.lab.heig-vd.ch
DNS	maltego.DNSName	intranet.heig-vd.ch
DNS	maltego.DNSName	media.heig-vd.ch
DNS	maltego.DNSName	imap.heig-vd.ch
DNS	maltego.DNSName	smtp.heig-vd.ch
DNS	maltego.DNSName	webmail.heig-vd.ch
DNS	maltego.DNSName	pop.heig-vd.ch
DNS	maltego.DNSName	proxy.heig-vd.ch
DNS	maltego.DNSName	trinity.heig-vd.ch
DNS	maltego.DNSName	morpheus.heig-vd.ch
DNS	maltego.DNSName	photos.heig-vd.ch
DNS	maltego.DNSName	www.heig-vd.ch
DNS	maltego.DNSName	ns1.heig-vd.ch
DNS	maltego.DNSName	mail01.heig-vd.ch
DNS	maltego.DNSName	mailcl5.heig-vd.ch
DNS	maltego.DNSName	vpn.heig-vd.ch
DNS	maltego.DNSName	oldmail.heig-vd.ch
DNS	maltego.DNSName	mailcl0.heig-vd.ch
DNS	maltego.DNSName	mailcl3.heig-vd.ch
DNS	maltego.DNSName	mailcl2.heig-vd.ch
DNS	maltego.DNSName	vpn2.heig-vd.ch
DNS	maltego.DNSName	mailcl4.heig-vd.ch
DNS	maltego.DNSName	mail02.heig-vd.ch
DNS	maltego.DNSName	netboxvpn.heig-vd.ch

- Des boîtes d'adresses mails

@ maltego.EmailAddress	noc@heig-vd.ch.
@ maltego.EmailAddress	rab@dmu.ac.uk
@ maltego.EmailAddress	mgongora@dmu.ac.uk
@ maltego.EmailAddress	taillard@crt.umontreal.ca
@ maltego.EmailAddress	elizondo@dmu.ac.uk
@ maltego.EmailAddress	eric@idsia.ch
@ maltego.EmailAddress	pluyima@dmu.ac.uk
@ maltego.EmailAddress	raoul.herzog@heig-vd.ch
@ maltego.EmailAddress	marcos.rubinstein@heig-vd.ch
@ maltego.EmailAddress	nathalie.nyffeler@heig-vd.ch
@ maltego.EmailAddress	anna.lupina-wegener@heig-vd.ch
@ maltego.EmailAddress	the-van.luong@heig-vd.ch
@ maltego.EmailAddress	international@heig-vd.ch
@ maltego.EmailAddress	matthieu.delapparent@heig-vd.ch
@ maltego.EmailAddress	yannick.arnould@heig-vd.ch
@ maltego.EmailAddress	gerhard.schneider@heig-vd.ch
@ maltego.EmailAddress	alberto.dassatti@heig-vd.ch
@ maltego.EmailAddress	eric.taillard@heig-vd.ch
@ maltego.EmailAddress	helpdesk@heig-vd.ch
@ maltego.EmailAddress	dorian.tille@heig-vd.ch
@ maltego.EmailAddress	ludovic.piquerez@heig-vd.ch
@ maltego.EmailAddress	david.cruchon@heig-vd.ch
@ maltego.EmailAddress	bastian.gardei@heig-vd.ch
@ maltego.EmailAddress	ludovic.maret@heig-vd.ch
@ maltego.EmailAddress	claude.philipona@heig-vd.ch
@ maltego.EmailAddress	arnaud.desclouds@heig-vd.ch
@ maltego.EmailAddress	christian.buchs@heig-vd.ch
@ maltego.EmailAddress	christopher.glass@heig-vd.ch
@ maltego.EmailAddress	alen.bijelic@heig-vd.ch
@ maltego.EmailAddress	joel.schar@heig-vd.ch
@ maltego.EmailAddress	philippe.waelti@heig-vd.ch
@ maltego.EmailAddress	laura.raileanu@heig-vd.ch
@ maltego.EmailAddress	contact@idfm98.fr
@ maltego.EmailAddress	infos@idfm98.fr
@ maltego.EmailAddress	silog.fr@free.fr
@ maltego.EmailAddress	david.cruchon@komeres.fr
@ maltego.EmailAddress	rnollan@gmail.com
@ maltego.EmailAddress	more@usphonebook.com
@ maltego.EmailAddress	free@rocketreach.co
@ maltego.EmailAddress	contact@komeres.fr
@ maltego.EmailAddress	pecran@cerens.fr
@ maltego.EmailAddress	david.cruchon@syselcloud.ch
@ maltego.EmailAddress	david@enophi.ch

- 2 Adresses ipv4

 maltego.IPv4Address	193.134.218.124
 maltego.IPv4Address	145.232.233.54

- 2 MX record - entrée DNS pour des serveurs mails

 maltego.MXRecord	gwsmtpl1.avdtec.ch
 maltego.MXRecord	mail01.heig-vd.ch

- 6 Netblock - “A range of IP versions 4 addresses” d’après la documentation

 maltego.Netblock	27.126.146.0-27.126.146.255
 maltego.Netblock	103.28.42.0-103.28.42.255
 maltego.Netblock	203.55.21.0-203.55.21.255
 maltego.Netblock	204.75.142.0-204.75.142.255
 maltego.Netblock	146.88.28.0-146.88.28.255
 maltego.Netblock	163.47.180.0-163.47.183.255

- 7 NS (Name Server) record - qui identifient les serveurs responsables de zones DNS

 maltego.NSRecord	ns-459.awsdns-57.com
 maltego.NSRecord	scsnms.switch.ch
 maltego.NSRecord	ns-811.awsdns-37.net
 maltego.NSRecord	ns-1308.awsdns-35.org
 maltego.NSRecord	ns-2025.awsdns-61.co.uk
 maltego.NSRecord	ns02.heig-vd.ch
 maltego.NSRecord	ns01.heig-vd.ch

- Des Personnes - qui devraient correspondre à des gens ayant un lien avec le domaine heig-vd.ch

 maltego.Person	Ludovic Maret
 maltego.Person	Christian Buchs
 maltego.Person	Tille Dorian
 maltego.Person	Claude Philipona
 maltego.Person	Bastian Gardel
 maltego.Person	Alen Bijelic
 maltego.Person	Joel Schär
 maltego.Person	Arnaud Desclouds
 maltego.Person	Christopher Glass
 maltego.Person	Philippe Waelti
 maltego.Person	David Cruchon
 maltego.Person	Ludovic Piquerez
 maltego.Person	Laura Raileanu

- Des numéros de téléphone - toujours en lien avec le nom de domaine

 maltego.PhoneNumber	+41 24 557 63 30
 maltego.PhoneNumber	24 557 61 60
 maltego.PhoneNumber	+41 24 557 27 81
 maltego.PhoneNumber	+41 24 557 75 90
 maltego.PhoneNumber	+41 21 693 76 48
 maltego.PhoneNumber	+41 21 693 25 45
 maltego.PhoneNumber	24 557 62 64
 maltego.PhoneNumber	+41 24 557 62 99
 maltego.PhoneNumber	+41 24 557 62 76
 maltego.PhoneNumber	+41 24 557 62 79
 maltego.PhoneNumber	+41 24 557 73 70
 maltego.PhoneNumber	+41 24 557 76 12
 maltego.PhoneNumber	+06 07 26 00 66
 maltego.PhoneNumber	+01 34 12 12 22
 maltego.PhoneNumber	10 05 2019
 maltego.PhoneNumber	617 570 2618
 maltego.PhoneNumber	29 11 2018
 maltego.PhoneNumber	01 05 2018
 maltego.PhoneNumber	28 09 2020
 maltego.PhoneNumber	10 02 2021
 maltego.PhoneNumber	11 01 2021
 maltego.PhoneNumber	12 12 2020
 maltego.PhoneNumber	05 12 2020
 maltego.PhoneNumber	01 12 2020

- Lien sur des captures “Snapshots wayback machine”

maltego.wayback.Snapshot	2014 Sep 29: http://iae.heig-vd.ch:80/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2Ffr%2Dch%2FEnseignement%2FSupports%2F
maltego.wayback.Snapshot	2010 Oct 24: http://www.iae.heig-vd.ch:80/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2Ffr%2Dch%2FEnseignement%2FSupports%2F
maltego.wayback.Snapshot	2016 Mar 27: http://iae.heig-vd.ch/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2ffr%2Dch%2fEnseignement%2fSupports%2F
maltego.wayback.Snapshot	2010 Jul 17: http://www.iae.heig-vd.ch:80/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2Ffr%2Dch%2FEnseignement%2FSupports%2F
maltego.wayback.Snapshot	2016 Aug 26: http://iae.heig-vd.ch/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2ffr%2Dch%2fEnseignement%2fSupports%2F
maltego.wayback.Snapshot	2014 Sep 29: http://iae.heig-vd.ch:80/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2Ffr%2Dch%2FEnseignement%2FSupports%2F
maltego.wayback.Snapshot	2010 Jul 17: http://www.iae.heig-vd.ch:80/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2Ffr%2Dch%2FEnseignement%2FSupports%2F
maltego.wayback.Snapshot	2013 Nov 19: http://www.iae.heig-vd.ch:80/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2Ffr%2Dch%2FEnseignement%2FSupports%2F
maltego.wayback.Snapshot	2013 Nov 18: http://www.iae.heig-vd.ch:80/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2Ffr%2Dch%2FEnseignement%2FSupports%2F
maltego.wayback.Snapshot	2013 Jan 15: http://iae.heig-vd.ch:80/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2Ffr%2Dch%2FEnseignement%2FSupports%2F
maltego.wayback.Snapshot	2016 Aug 21: http://iae.heig-vd.ch/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2ffr%2Dch%2fEnseignement%2fSupports%2F
maltego.wayback.Snapshot	2016 Mar 27: http://iae.heig-vd.ch/fr-ch/Enseignement/Supports/Forms/AllItems.aspx?RootFolder=%2ffr%2Dch%2fEnseignement%2fSupports%2F
maltego.wayback.Snapshot	2008 May 29: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2008 Dec 11: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2007 Mar 04: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2006 Dec 19: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2006 Aug 15: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2008 May 02: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2008 Mar 12: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2007 Oct 14: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2022 Jan 20: http://iese.heig-vd.ch/Telerik.Web.UI.WebResource.axd?compress=0&_TSM_CombinedScripts_=%%3b%%3bTelerik.Sitefinity.Resources%
maltego.wayback.Snapshot	2009 May 03: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2008 Feb 06: http://iese.heig-vd.ch:80/training
maltego.wayback.Snapshot	2006 Aug 15: http://iese.heig-vd.ch:80/training

- Des domaines

maltego.Domain	spf.hefr.ch
maltego.Domain	aspmx.pardot.com
maltego.Domain	heig-vd.health
maltego.Domain	heig-vd.com
maltego.Domain	heig-vd.live
maltego.Domain	heig-vd.top
maltego.Domain	heig-vd.org
maltego.Domain	heig-vd.site
maltego.Domain	heig-vd.ch

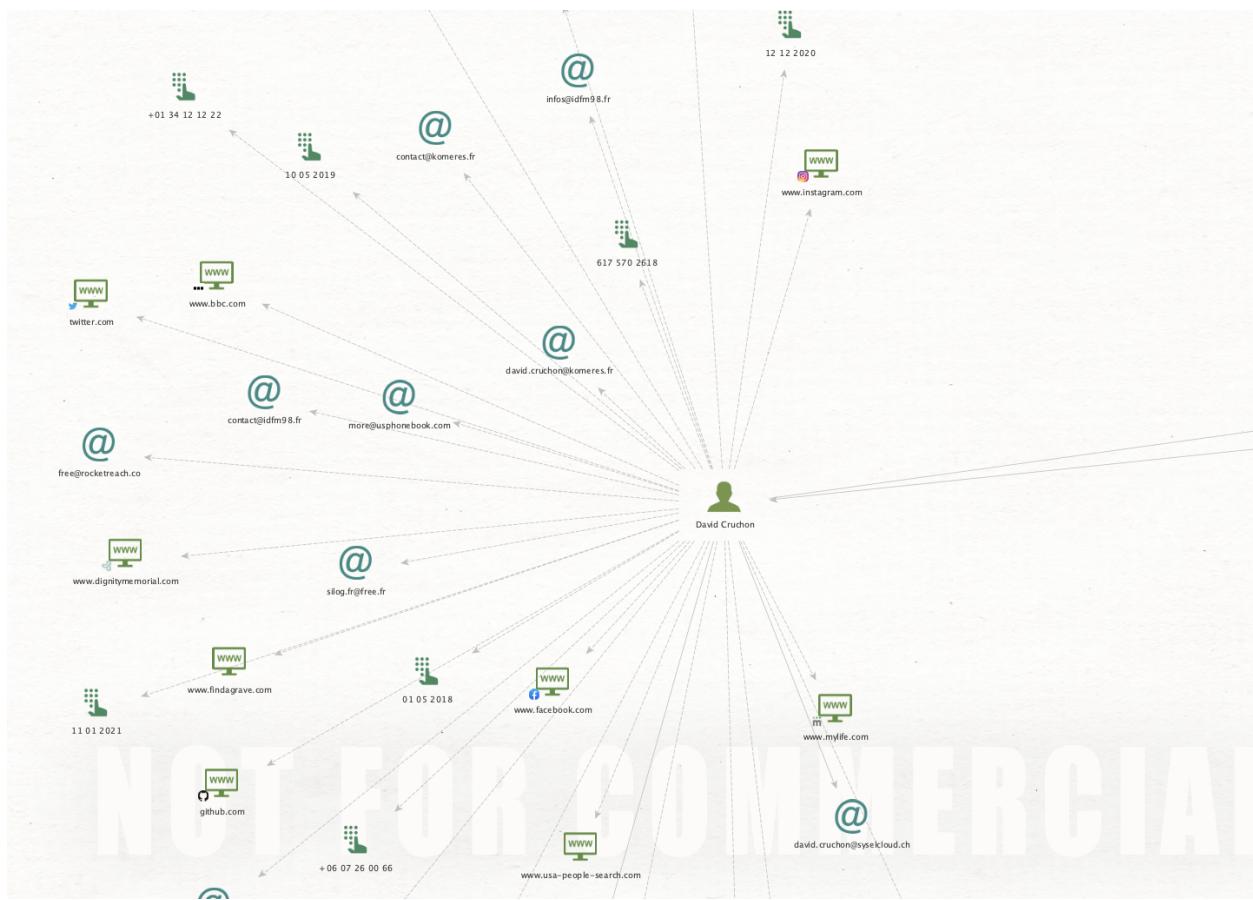
- Et des URLs de site web

💻 maltego.Website	lict-space.heig-vd.ch
💻 maltego.Website	reds.heig-vd.ch
💻 maltego.Website	iai.heig-vd.ch
💻 maltego.Website	smapshot.heig-vd.ch
💻 maltego.Website	reds-data.heig-vd.ch
💻 maltego.Website	php.iai.heig-vd.ch
💻 maltego.Website	heig-vd.ch
💻 maltego.Website	gaps.heig-vd.ch
💻 maltego.Website	contacts.heig-vd.ch
💻 maltego.Website	www.osti.gov
💻 maltego.Website	assolegnorisponde.it
💻 maltego.Website	www.researchgate.net
💻 maltego.Website	cours-examens.org
💻 maltego.Website	www.fpl2016.org
💻 maltego.Website	en.wikipedia.org
💻 maltego.Website	www.academia.edu
💻 maltego.Website	www.buildsoft.eu
💻 maltego.Website	jmlr.csail.mit.edu
💻 maltego.Website	china-in-europe.net
💻 maltego.Website	www.hes-so.ch
💻 maltego.Website	www.vd.ch
💻 maltego.Website	www.heig-vd.ch
💻 maltego.Website	mistic.heig-vd.ch
💻 maltego.Website	davidcrichton.ca
💻 maltego.Website	twitter.com
💻 maltego.Website	www.findagrave.com
💻 maltego.Website	www.linkedin.com
💻 maltego.Website	www.dignitymemorial.com
💻 maltego.Website	github.com
💻 maltego.Website	www.facebook.com
💻 maltego.Website	www.ancientfaces.com
💻 maltego.Website	www.instagram.com
💻 maltego.Website	www.mylife.com
💻 maltego.Website	www.bbc.com
💻 maltego.Website	www.usa-people-search.com

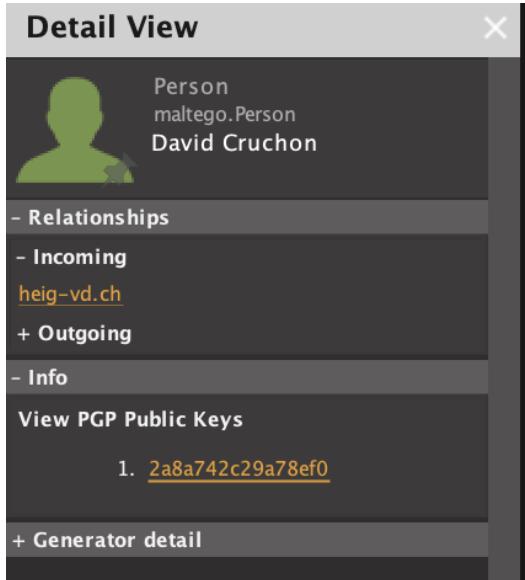
Au premier coup d'œil, aucune entité ne semble compromettante pour l'école (aucune adresse de crypto monnaie, de CVE ou de service douteux). On note cependant que beaucoup d'adresses mails ne semblent pas directement rattachées à l'école. Il en est de même pour les numéros de téléphone, dont la moitié ont un préfixe étranger.

## Analyse d'une identité

Nous allons nous pencher sur l'analyse d'une personne: **David Cruchon**. Cette personne a été sélectionnée aléatoirement, et est reliée au domaine heig-vd.ch via une entité profil et une adresse mail (les deux arêtes adjacentes au sommet profil, à droite de ce dernier sur la capture ci-dessous).



Si nous cherchons une vue détaillée du profil, nous constatons que le profil est construit sur la base d'une clef PGP [sourcée sur le site suivant](#) (lien “View PGP Public Keys” sur l'image suivante).



Nous pouvons supposer que David Cruchon est un prénom et un nom relativement courant, pouvant donc être commun à plusieurs personnes différentes. Nous souhaitons donc nous assurer qu'il s'agisse bien d'une personne ayant un lien quelconque avec la HEIG-VD.

Pour ce faire, nous lançons une nouvelle recherche à partir du profil de David Cruchon.

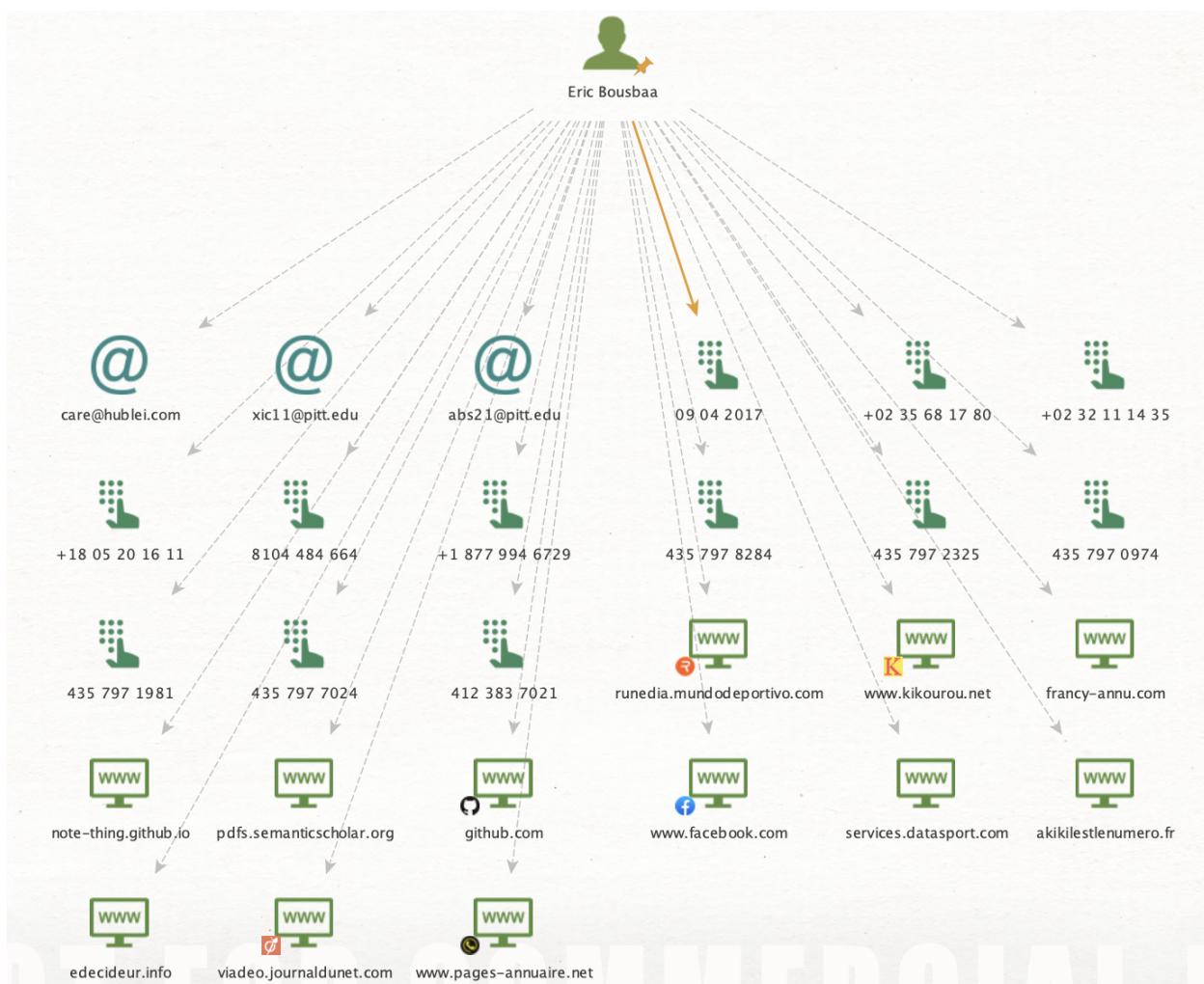
Dans les website associés à l'identité, nous obtenons un [compte Github](#). Au vu des repositories publics créés, (CLD-Project-AWSRekog (créé en 2020, Teaching-HEIGVD-RES-2019-Exercise-Calculator, MAC-PROJECT (créé en 2020))), nous pouvons supposer qu'il s'agit d'un étudiant en TIC, présent dans la filière IL. N'étant plus dans la liste d'élèves présent sur Gaps, nous pouvons supposer que ce dernier a terminé son cursus en 2021

## Recherche d'une identité

### Identité 1 - Eric Bousbaa (moi)

En me cherchant moi-même j'obtiens une 3 adresses mails, une liste de numéros de téléphones aléatoires, quelques résultats sportifs d'évènements de course à pied, qui font bien référence à moi (même si le site "kirikou.net" est un peu raciste, mais passons), ainsi que mon Github.

J'obtiens également des sites web d'annuaires, principalement français qui ne semblent contenir aucune information me concernant.



Plus spécifiquement, les adresses mails trouvées sont les suivantes :

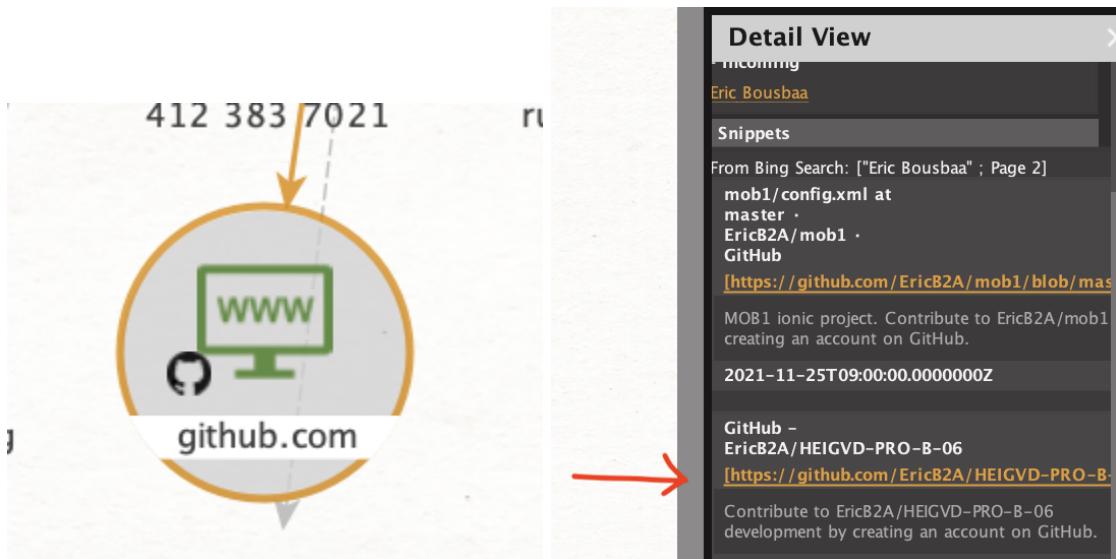


- [care@hublei.com](mailto:care@hublei.com) : il s'agirait d'une entreprise en Inde qui vend des produits en lignes fait mains . Le moteur de recherche Bing semblerait faire un lien entre mon identité et une adresse email présente sur leur site web.



- [xic11@pitt.edu](mailto:xic11@pitt.edu) : Toujours Bing qui fait référence à cette adresse email, qui appartiendrait au domaine engineering de l'université de Pittsburg. Même si je suis convaincu que Pitt est une université très intéressante, je n'ai aucun lien avec cette école.
- [abs12@pitt.edu](mailto:abs12@pitt.edu) : Cas identique à l'adresse email précédente.

Donc en soit, rien de pertinent. Pourtant, il suffirait de parcourir le README de mes repository Github **mentionné dans mes sites web retrouvés** pour trouver mon adresse email, dans le cas ci-dessous appartenant à la HEIG-VD.

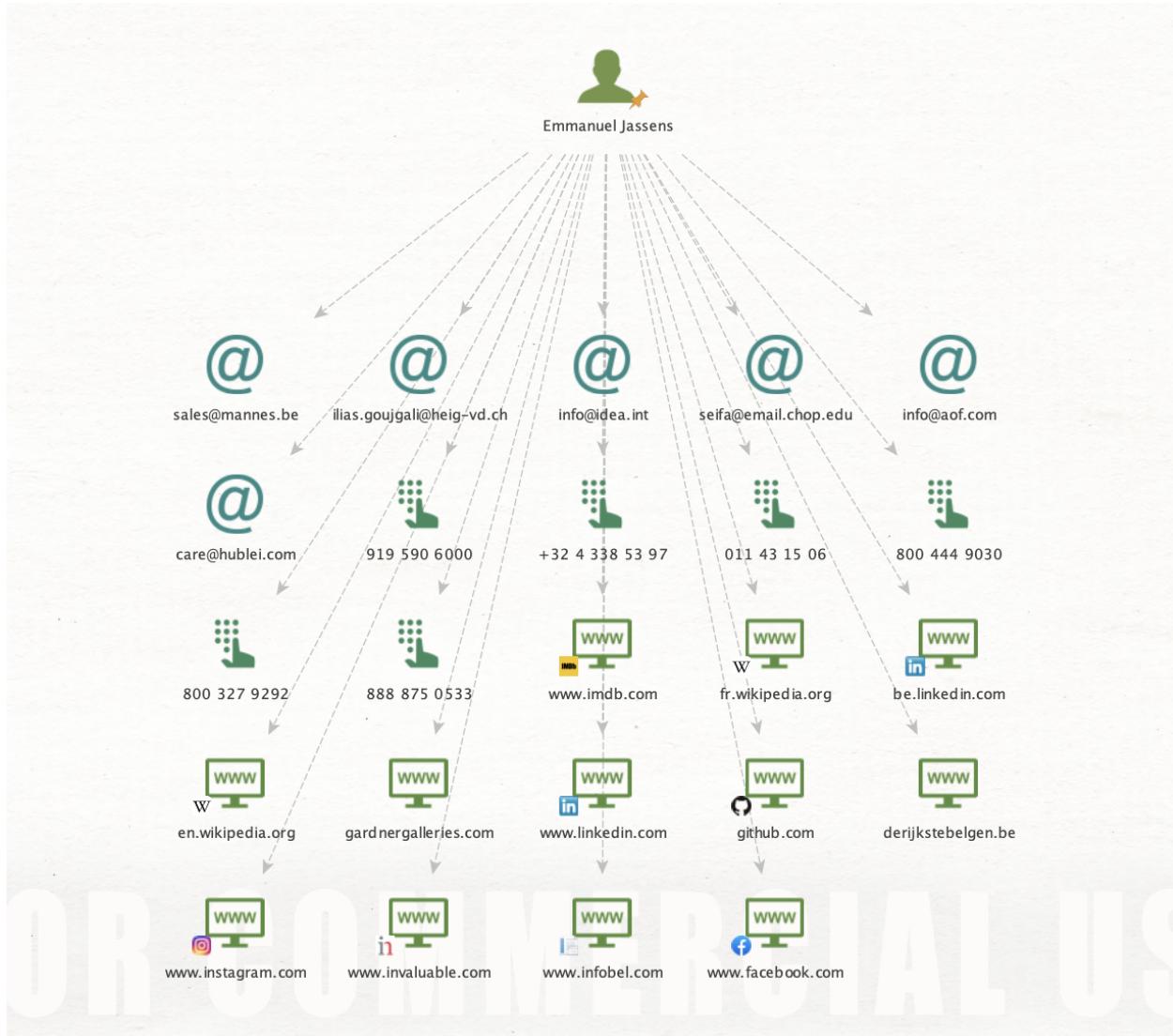


## GROUPE B-06

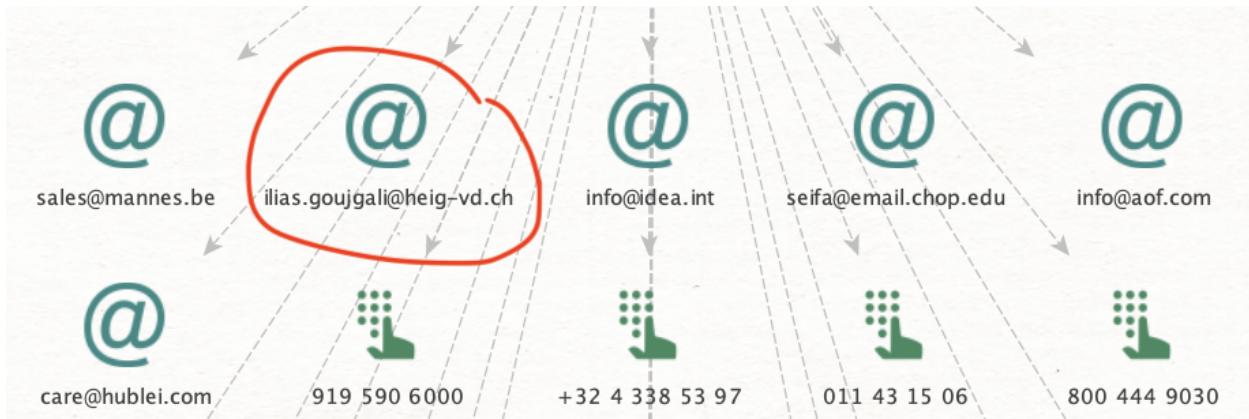
prénom nom	email	github
Eric Bousbaa (chef de projet)	eric.bousbaa@heig-vd.ch	EricBroutba
Thibaud Franchetti (remplaçant chef de projet)	thibaud.franchetti@heig-vd.ch	ChatDeBlofeld
Gildas Houlmann	gildas.houlmann@heig-vd.ch	G-Houlmann
Guillaume Laubscher	guillaume.laubscher@heig-vd.ch	BuildTools
Alexandre Simik	alexandre.simik@heig-vd.ch	Moromir
Christian Zaccaria	christian.zaccaria@heig-vd.ch	zaccariach

## Identité 2 - Emmanuel Jassens

En voulant montrer Maltego à un camarade de classe, j'ai effectué une recherche sur lui.



Toujours intéressé par l'adresse email, il est amusant de constater que cette fois une adresse email venant du répertoire Github du même cours (PRO, semestre 4 de la HEIG-VD) a été trouvée.



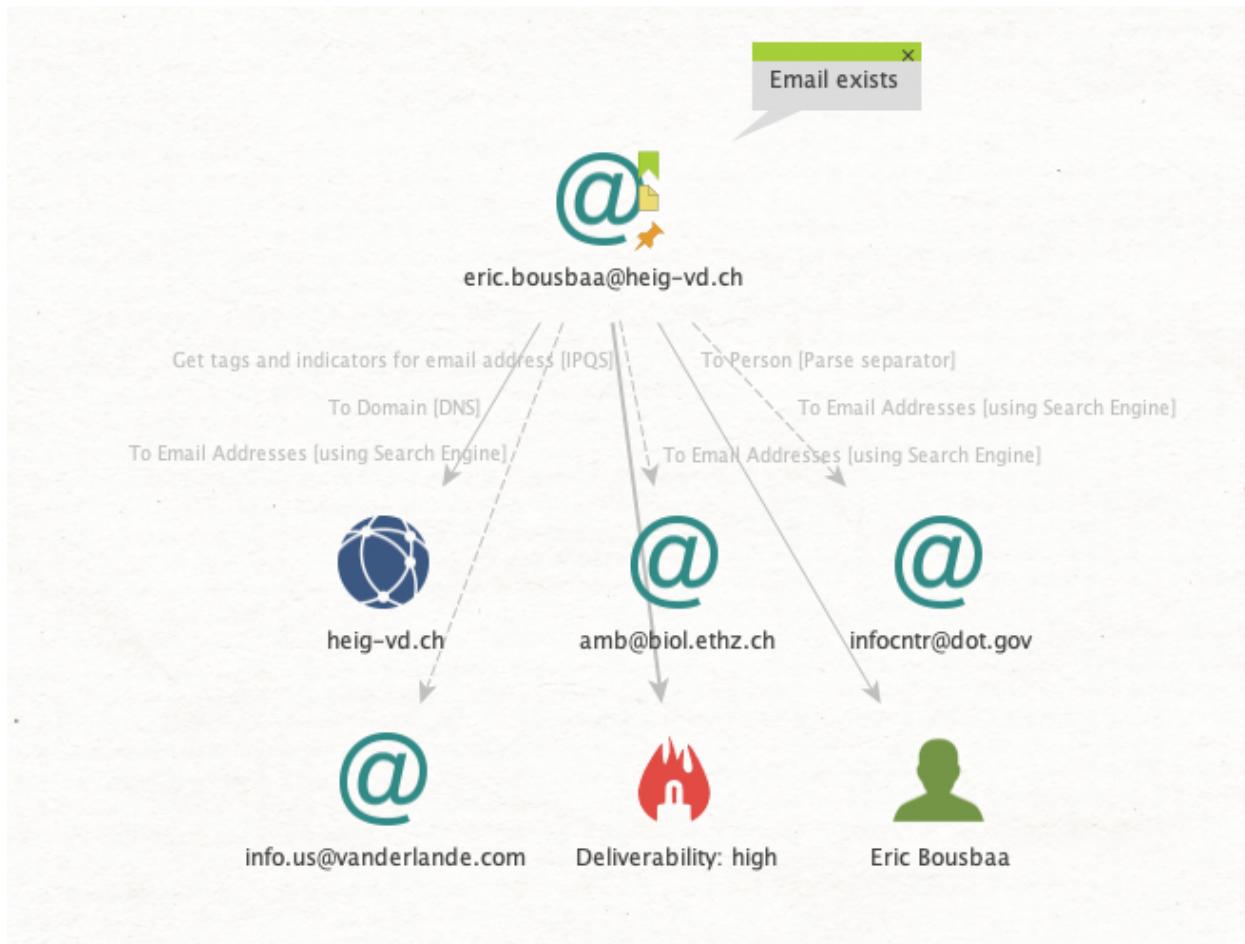
Cependant, il s'agit d'une adresse email de l'un de ses camarades, Ilias Goujgali. La sienne étant présente juste en dessous.

Development team:

Name	Email	Github
Goujgali Ilias (project lead)	<a href="mailto:ilias.goujgali@heig-vd.ch">ilias.goujgali@heig-vd.ch</a>	Double-i
Janssens Emmanuel (deputy project lead)	<a href="mailto:emmanuel.janssens@heig-vd.ch">emmanuel.janssens@heig-vd.ch</a>	emmanueljanssens
Vaz Afonzo Vitor	<a href="mailto:vitor.vazafonzo@heig-vd.ch">vitor.vazafonzo@heig-vd.ch</a>	vitorva
Potet Bastien	<a href="mailto:bastien.potet@heig-vd.ch">bastien.potet@heig-vd.ch</a>	Bpotet
Lehmann Maurice	<a href="mailto:maurice.lehmann@heig-vd.ch">maurice.lehmann@heig-vd.ch</a>	mauricelehmann
Reuteler Robin	<a href="mailto:robin.reuteler@heig-vd.ch">robin.reuteler@heig-vd.ch</a>	reutelerr

## Recherche d'une adresse mail

En effectuant une recherche avec mon adresse mail heig-vd.ch (en lien avec l'organisation précédemment cherché), on constate que l'adresse est rapidement associée au nom de domaine heig-vd.ch ainsi qu'à mon identité.



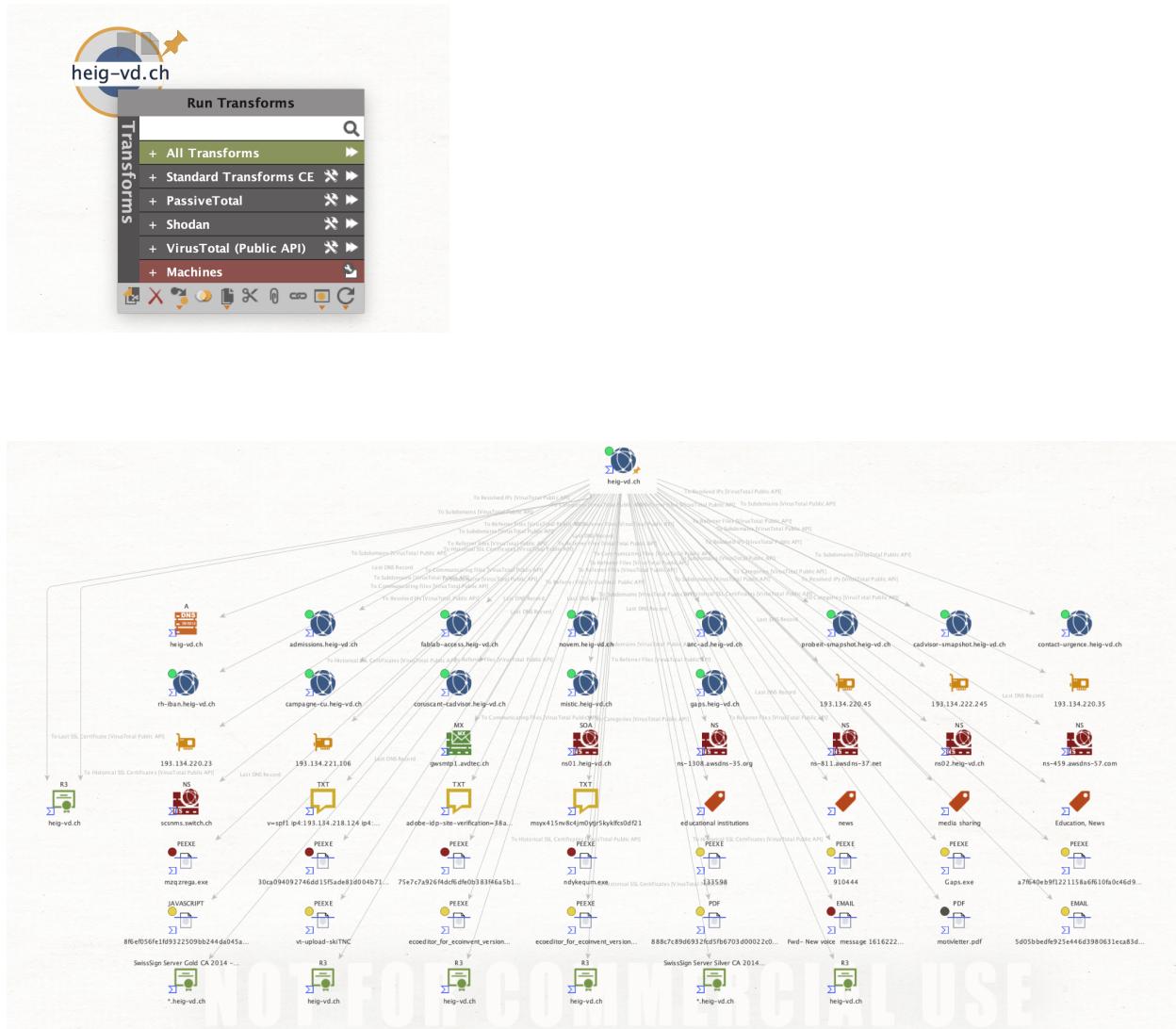
On remarque également un “Deliverability : high” , qui d’après la documentation de Maltego indique le niveau de fraude de l’adresse mail. Ou dit autrement, quelles sont les chances que l’adresse existe réellement.

# Installation et utilisation de nouvelles transformations

## VirusTotal

### Reconnaissance d'un domaine

Nous effectuons une recherche sur le même domaine précédent, heig-vd.ch, en partant d'une entité Domain.



En plus des noms de domaines et adresses IPV4 trouvés par les transformations de base de Maltego, VirusTotal nous fournit les informations suivantes :

- Des fichiers - dont des fichiers WIN.EXE, des fichiers eml (liés aux mail), des pdf ou encore des fichiers javascripts.

maltego.virustotal.File	mzqzrega.exe
maltego.virustotal.File	30ca094092746dd15f5ade81d004b712_kaf
maltego.virustotal.File	75e7c7a926f4dcf6dfe0b383f46a5b19576d1fd47aee30db07a64998fd7675be.exe
maltego.virustotal.File	ndykequm.exe
maltego.virustotal.File	133598
maltego.virustotal.File	910444
maltego.virustotal.File	Gaps.exe
maltego.virustotal.File	a7f640eb9f1221158a6f610fa0c46d92d762a38571b616ad283b46e88e48ed48
maltego.virustotal.File	8f6ef056fe1fd9322509bb244da045a191f6bbf7215f13d0178bdb1d7404b90
maltego.virustotal.File	vt-upload-skiTNC
maltego.virustotal.File	ecoeditor_for_ecoinvent_version_3v3.7.200.14330.exe
maltego.virustotal.File	ecoeditor_for_ecoinvent_version_3v3.8.600.15190.exe
maltego.virustotal.File	888c7c89d6932fcdf5fb6703d00022c08048a311c90b5d1479b1cffa2960700d5
maltego.virustotal.File	Fwd- New voice message 16162220248 in mailbox 161622202481 from %2216162220248%22 <6804549986>.eml
maltego.virustotal.File	motivletter.pdf
maltego.virustotal.File	5d05bbbedfe925e446d3980631eca83deec4c6a3a3234dd28b75614b022df3c12

- Des phrases - qui correspondent à du texte trouvé.

maltego.Phrase	v=spf1 ip4:193.134.218.124 ip4:145.232.233.54 ip4:27.126.146.0/24 ip4:103.28.42.0/24 ip4:146.88.28.0/24 ip4:163.47.180.0/22 ip4:203
maltego.Phrase	adobe-idp-site-verification=38a35c2c3cc6e86da35b8375404692f367713de605009c52e448eb39368c1203
maltego.Phrase	msyx415nv8c4jm0ytjr5kyklfcs0df21

- Et pour finir des certificats X509 liés au domaine heig-vd.ch

maltego.X509Certificate	heig-vd.ch
maltego.X509Certificate	*.heig-vd.ch
maltego.X509Certificate	heig-vd.ch
maltego.X509Certificate	heig-vd.ch
maltego.X509Certificate	heig-vd.ch
maltego.X509Certificate	*.heig-vd.ch
maltego.X509Certificate	heig-vd.ch

Les fichiers exécutables sont les éléments les plus intéressants (à mon sens). Cependant, même si la transformation permet de trouver certaines informations concernant un fichier, l'emplacement de ce dernier n'est pas retourné.

## Recherche d'une identité

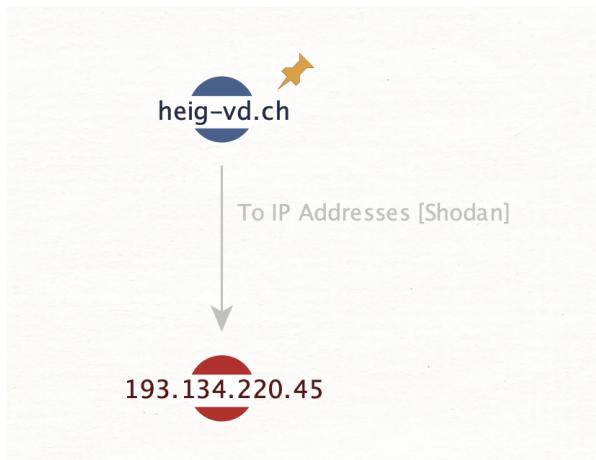
VirusTotal n'offre malheureusement pas de transformations sur les Entités identité ou adresse email.



## Shodan

### Reconnaissance d'un domaine

Shodan est un moteur de recherche pour types de serveurs connectés à internet (objets connectés, serveurs, services, etc...). En effectuant une recherche sur le domaine heig-vd.ch, nous obtenons l'adresse ip ci-dessous.



En effectuant une simple recherche whois, nous constatons qu'il s'agit bel et bien d'une adresse ip rattachée à l'école

```
person:          Fabrice Demierre
address:        Route de Cheseaux 1
address:        1401
address:        Yverdon-les-Bains
address:        SWITZERLAND
phone:          +41 24 557 64 43
nic-hdl:        FD5193-RIPE
mnt-by:         ch-heig-vd-1-mnt
created:        2016-03-17T08:28:25Z
last-modified:  2016-03-17T08:28:26Z
source:         RIPE
```

L'ip est pingable mais ne répond pas à une requête HTTP.

Shodan ne fournit aucune information supplémentaire sur l'adresse IP.

The screenshot shows the Shodan search interface. At the top, there are three colored status indicators (red, grey, green) followed by the word "Details". Below the status indicators is a navigation bar with tabs: "Summary", "Attachments (0)", "Notes", and "Properties (2)". The "Properties (2)" tab is currently selected. In the main content area, there is a single property entry: "IP Address 193.134.220.45" and below it, the label "Internal" with a small checkbox next to it.

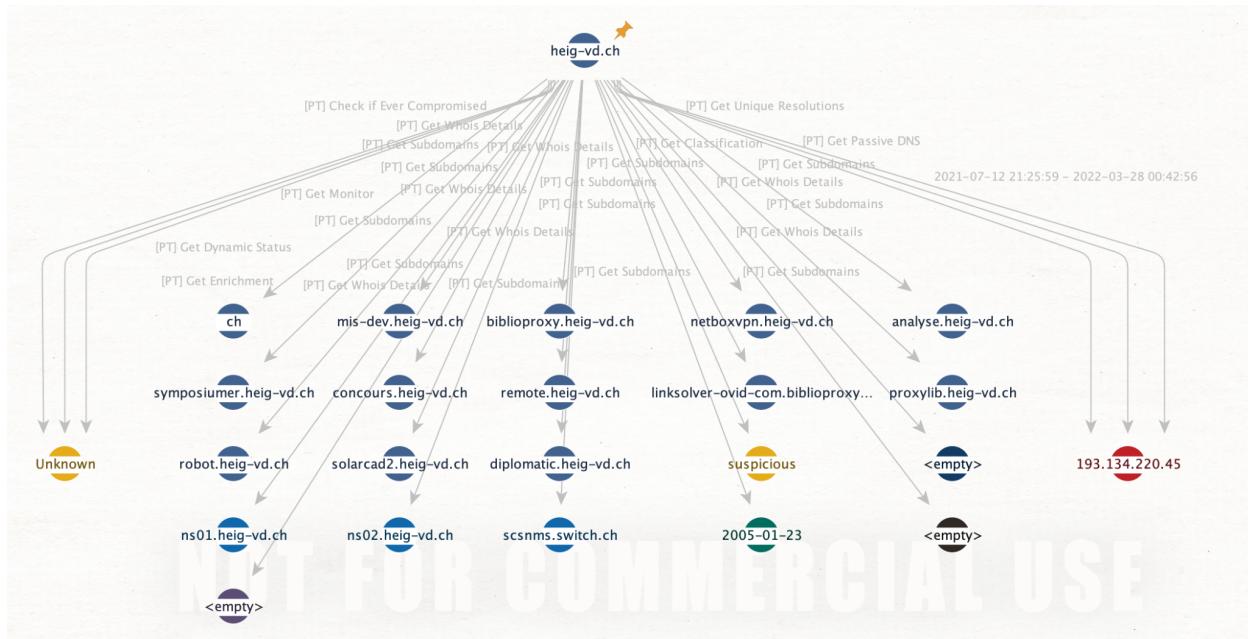
### Recherche d'une identité

Tout comme VirusTotal, Shodan ne permet pas d'effectuer des transformations sur les entités d'une personne ou d'une adresse email.

## PassiveTotal

### Reconnaissance d'un domaine

PassiveTotal, décrit comme un analyseur de sécurité, nous fournit les informations suivantes sur le domaine heig-vd.ch



PassiveTotal parvient à trouver quelques noms de domaine en plus de la transformation de base de Maltego, tel que `diplomatic.heig-vd.ch` ou encore `robot.heig-vd.ch`

maltego.Domain	ch
maltego.Domain	heig-vd.ch
maltego.Domain	mis-dev.heig-vd.ch
maltego.Domain	biblioproxy.heig-vd.ch
maltego.Domain	netboxvpn.heig-vd.ch
maltego.Domain	analyse.heig-vd.ch
maltego.Domain	symposiumer.heig-vd.ch
maltego.Domain	concours.heig-vd.ch
maltego.Domain	remote.heig-vd.ch
maltego.Domain	linksolver-ovid-com.biblioproxy.heig-vd.ch
maltego.Domain	proxylib.heig-vd.ch
maltego.Domain	robot.heig-vd.ch
maltego.Domain	solarcad2.heig-vd.ch
maltego.Domain	diplomatic.heig-vd.ch

Cette transformation ne retourne cependant aucune information concernant des identités ou adresses mails. Donc même si la recherche semble plus précise, le spectre d'éléments recherchés est lui moins large.

On y trouve également la même adresse IP que Shodan.

 maltego.IPV4Address	193.134.220.45
---	----------------

Deux phrases, ne contenant aucune information de plus que “suspicious” ou “unknown”.

 maltego.Phrase	Unknown
 maltego.Phrase	suspicious

Ainsi que des records whois.

 pt.whoisExpiresAt	
 pt.whoisNameserver	ns01.heig-vd.ch
 pt.whoisNameserver	ns02.heig-vd.ch
 pt.whoisNameserver	scsnms.switch.ch
 pt.whoisRegistered	2005-01-23
 pt.whoisRegistrar	
 pt.whoisRegistryUpdatedAt	

---

## Recherche d'une adresse mail

PassiveTotal ne permet pas d'effectuer une transformation sur une Personne. Cependant, on peut le faire sur une adresse mail. Nous allons donc effectuer une recherche sur mon adresse mail, liée au domaine heig-vd du point précédent.



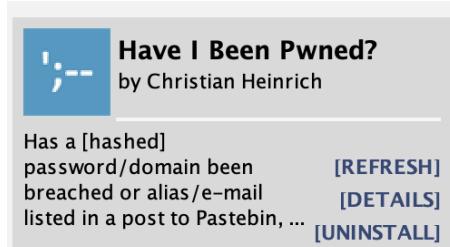
Miséricorde ! Aucune information n'est trouvée à partir de cette adresse mail ! Ceci vient confirmer notre supposition : PassiveTotal, bien que plus précis qu'une recherche Maltego de base, effectue des recherches moins larges. Il serait donc judicieux de commencer par une recherche "Maltego vanilla" puis de s'attarder sur des recherches PassiveTotal.

## Et maintenant ?

Nous allons maintenant nous pencher sur trois transformations gratuites :

Transformation	Description
Have I been pwned	Permet de savoir si nos données personnelles ont été compromises
URLhaus	Projet ayant pour but de collecter, traquer des malwares.
Google programmable search engine	Analyse la présence d'une personne sur les réseaux sociaux

### Have I been pwned



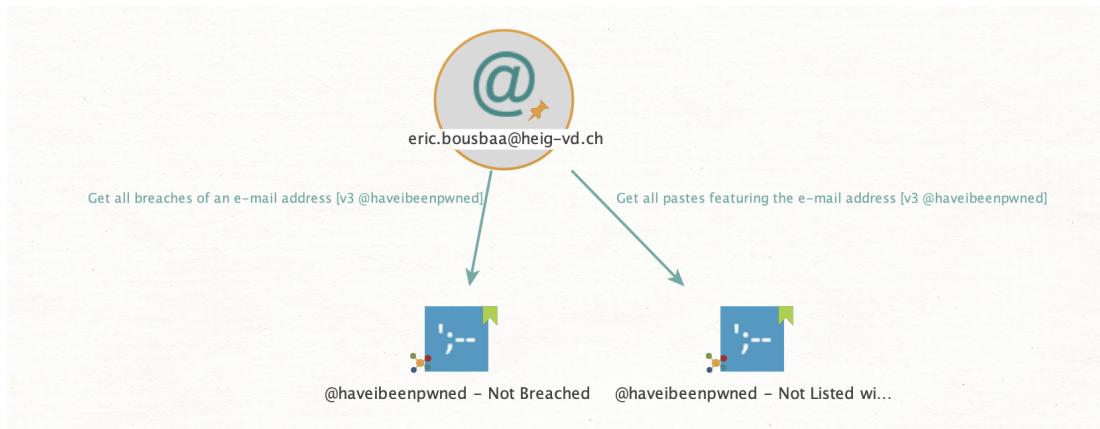
### Reconnaissance d'un domaine



Il s'agit là d'une bonne nouvelle, Have I Been Pwned ne trouve aucune information concernant le domaine de la heig-vd.

## Recherche d'une identité

Cependant, en lançant la même transformation sur mon adresse reliée au site de la heig-vd, nous obtenons deux résultats.



Le premier indique “No breached”, ce qui signifie selon la documentation de Have I Been Pwned<sup>1</sup> que l’adresse email n’est présente dans aucune faille connue.

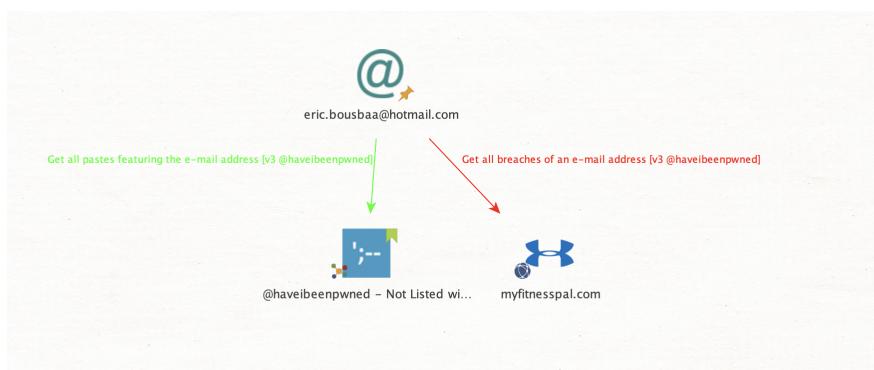
Le second élément indique “Not Listed within Pastes”, c’est à dire que l’adresse email n’a pas été “copiée” sur un site web public, qui pourrait potentiellement être récupéré par une personne malveillante.

Par soucis de complétude, j’ai essayé de lancer la même recherche sur mon adresse email privée “poubelle”, que j’ai tendance à utiliser sans me soucier de recevoir des spams ou que cette dernière soit compromise.

J’ai été surpris de constater qu’en plus de 10 ans d’utilisation, la seule brèche répertoriée est myFitnesspal.

Il s’agirait d’une brèche remontant à 2018<sup>2</sup>. J’espère n’avoir pas réutilisé le même mot de passe depuis.

Le seul nouveau type retourné par la transformation est “Node”, qui est assez générique et nous informe du statut de l’adresse (compromis, sur site public, etc..).



<sup>1</sup> <https://haveibeenpwned.com/FAQs>

<sup>2</sup> <https://fortune.com/2019/02/14/hacked-myfitnesspal-data-sale-dark-web-one-year-breach/>

## Urlhaus.abuse.ch



### Reconnaissance d'un domaine

Il serait intéressant de pousser la recherche d'URL, notamment sur les fichiers trouvés par VirusTotal, afin de trouver une intersection entre les fichiers de VirusTotal et un potentiel logiciel malveillant



Cependant, la transformation ne trouve aucun document, ce qui est une bonne nouvelle.

### Recherche d'une identité

UrlHause.abuse.ch ne permet pas d'effectuer de recherche sur une personne ou une adresse mail.

## Google programmable search engine

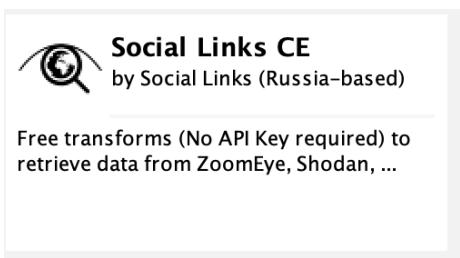


Il aurait été intéressant de s'intéresser quelque peu à des recherches de réseaux sociaux sur une personne ou une adresse email. Pour ce faire, la transformation “Google programmable search engine” aurait été adaptée.

Cependant, la transformation retourne toujours une erreur.

```
Running transform To MySpace profiles [Google] on 1 entities (from entity "Eric_Bousbaa")
Transform To Twitter profiles [Google] returned with an error: Internal server error. If you are the developer of these Transforms, please check the server logs (from entity "Eric_Bousbaa")
Transform To Reddit profiles [Google] returned with an error: Internal server error. If you are the developer of these Transforms, please check the server logs (from entity "Eric_Bousbaa")
Transform To Facebook profiles [Google] returned with an error: Internal server error. If you are the developer of these Transforms, please check the server logs (from entity "Eric_Bousbaa")
Transform To MySpace profiles [Google] returned with an error: Internal server error. If you are the developer of these Transforms, please check the server logs (from entity "Eric_Bousbaa")
Transform To GitHub profiles [Google] returned with an error: Internal server error. If you are the developer of these Transforms, please check the server logs (from entity "Eric_Bousbaa")
Transform To GitHub profiles [Google] done (from entity "Eric_Bousbaa")
```

Une alternative de transformation concernant les réseaux sociaux proposée par Maltego serait Social Link CE.



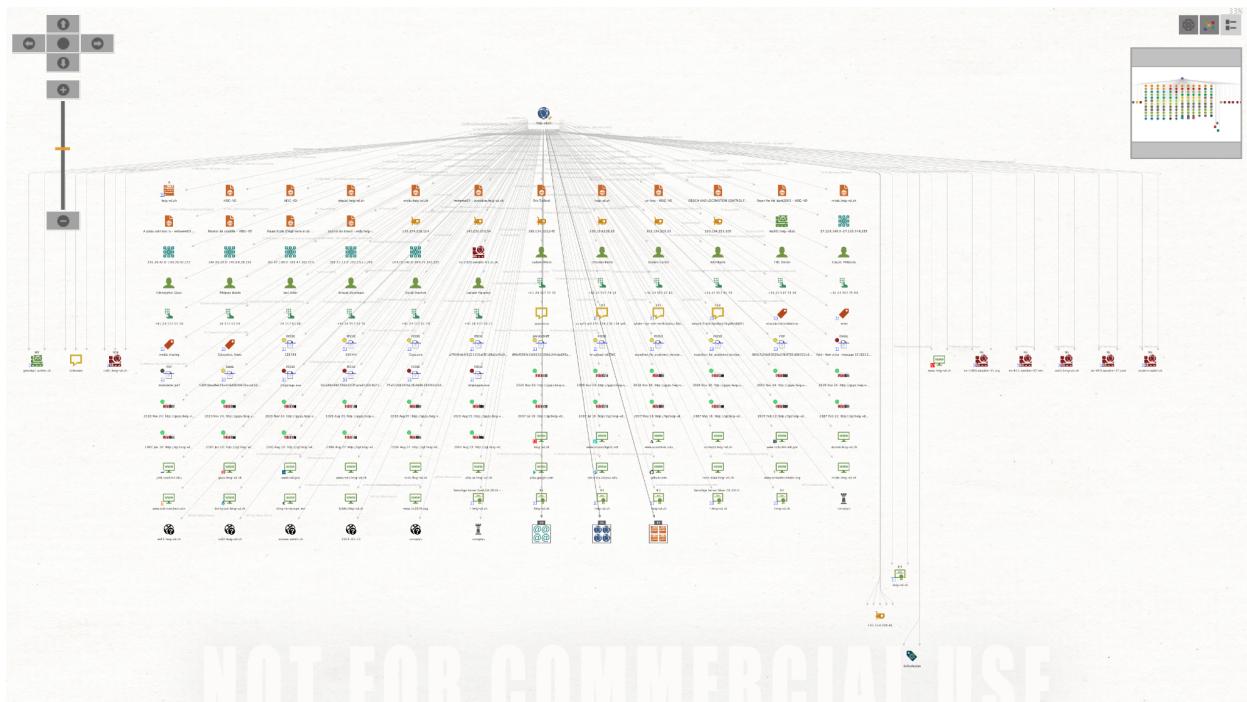
Cependant, celle-ci demande une clef API et étant basé en Russie, il serait imprudent de s'y enregistrer étant donné la situation politique du pays.

Ceci met en avant la dépendance de Maltego à des services externes. Ces derniers offrent des “Community Éditions” mais demandent de se créer un compte sur leur plateforme. Il est paradoxal d'entrer son adresse mail sur un site qui répertorie les adresses mails compromises.

## Conclusion

Maintenant que nous avons installé plusieurs transformations, que se passerait-il si nous décidions de toutes les lancer en même temps ?

Toujours sur la base du nom de domaine heig-vd.ch, nous obtenons le graphe suivant :



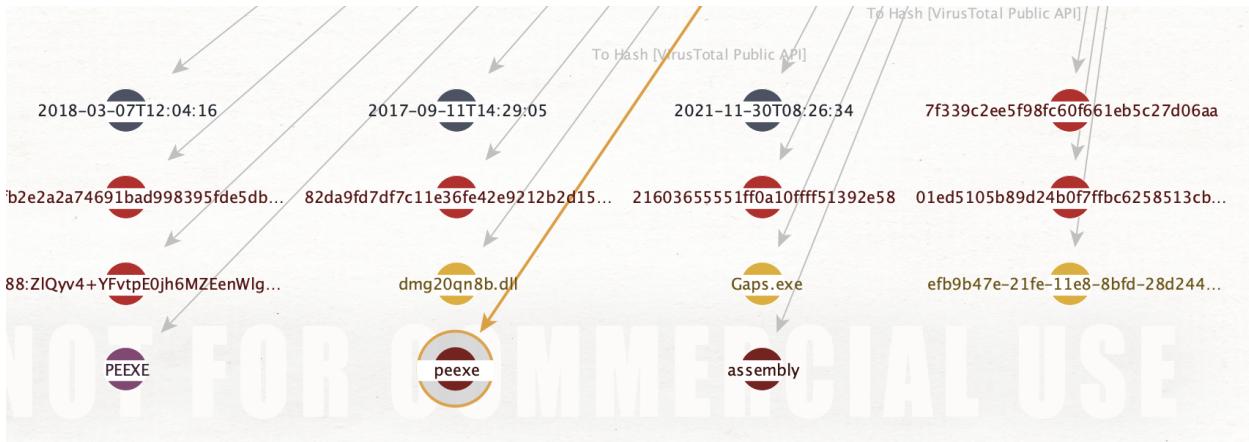
La représentation sous forme de graphe est difficile à comprendre, dû au nombre important de sommets du graphe. La “List View” est quelque peu plus digeste, mais donne un aperçu moins global du nombre de résultats trouvés.

Un fichier nommé “gaps.exe” attire mon attention.

Details	
Summary	Attachments (0)
Notes	Properties (24)
MeaningfulName	Gaps.exe
File Id	82da9fd7df7c11e36fe42e9212b2d1585309eb9a0f27d2749bf096006cf9f9be
Names	dmg20qn8b.dll, Gaps.exe, efb9b47e-21fe-11e8-8bfd-28d244a754d9
File Type	PEEXE
File Type Description	Win32 EXE
MDS	7f339c2ee5f98fc60f661eb5c27d06aa
SHA-1	0b4fb2e2a2a74691bad998395fde5db3faf2e362
SHA-256	82da9fd7df7c11e36fe42e9212b2d1585309eb9a0f27d2749bf096006cf9f9be
Vhash	21603655551ff0a10ffff51392e58
Authentihash	01ed5105b89d24b0f7ffbc6258513cb380b69855b6e1a632ab5f944d206861b4
SSDEEP	12288:ZlQyv4+YFvtPE0jh6MZEenWlg/ITasHG4vM:bQyEvt/h6XC2gSGE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 Mono/.Net assembly
File Size	1748992
Tags	peexe, assembly
Capability Tags	
Downloadable	null
Creation Date	2017-09-11T14:29:05Z
First Submission Date	2018-03-07T12:04:16Z
Last Submission Date	2018-03-07T12:04:16Z
Last Analysis Date	2021-11-30T08:26:34Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

Il aurait été intéressant de savoir où se trouve un tel fichier. Si ce même fichier était accessible, il pourrait s'agir d'une faille pour la heig-vd.ch. Quoiqu'il faut prendre avec des pincettes l'existence d'un tel fichier.

En lançant une seconde exécution depuis ce même fichier, en espérant y trouver plus d'informations, nous n'obtenons malheureusement aucune information exploitable.



Nous n'obtenons que des Phrases, des Hash, des types de fichiers ou encore de dates associés au fichier. Rien d'exploitable dans notre cas.

### Suggestion de transformation

Une suggestion de transformation serait de pouvoir retrouver des liens de parenté ou d'habitation avec d'autres personnes.

Par exemple, si je suis répertorié à "Altenhof Strasse 22, 1400, Yverdon, Switzerland" sur les pages blanches, il serait intéressant d'essayer de trouver d'autres personnes également enregistrées à la même adresse. Ainsi, on pourrait constituer le domicile d'une personne, ce qui est une information non négligeable pour du social engineering.

