

# Foot printing

## A. Troubleshooting réseaux

### Commande Ping

Pour trouver l'adresse IP de l'université Centrale, je lance un **ping** sur leur site :

```
C:\Users\nicos>ping www.universitecentrale.net

Envoi d'une requête 'ping' sur www.universitecentrale.net [188.165.51.130] avec 32 octets de données :
Réponse de 188.165.51.130 : octets=32 temps=107 ms TTL=51
Réponse de 188.165.51.130 : octets=32 temps=89 ms TTL=51
Réponse de 188.165.51.130 : octets=32 temps=93 ms TTL=51
Réponse de 188.165.51.130 : octets=32 temps=97 ms TTL=51

Statistiques Ping pour 188.165.51.130:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 89ms, Maximum = 107ms, Moyenne = 96ms
```

L'adresse est donc **188.165.51.130**

La taille du paquet IP est de **32 octets**

La commande **tracert** permet de montrer le chemin emprunter par le paquet ip jusqu'à sa destination.

```
C:\Users\nicos>tracert 188.165.51.130

Détermination de l'itinéraire vers ip130.ip-188-165-51.eu [188.165.51.130]
avec un maximum de 30 sauts :

 1  *      *      *      Délai d'attente de la demande dépassé.
 2  147 ms  75 ms  76 ms  10.96.0.1
 3  200 ms  97 ms  79 ms  192.168.254.30
 4   85 ms  78 ms  79 ms  192.168.255.58
 5  215 ms 128 ms  84 ms  194.149.164.102
 6  202 ms  93 ms  77 ms  194.149.166.13
 7  *      *      *      Délai d'attente de la demande dépassé.
 8  254 ms 117 ms  75 ms  be100.par-th2-pb1-nc5.fr.eu [213.186.32.181]
 9  *      *      *      Délai d'attente de la demande dépassé.
10  *      *      *      Délai d'attente de la demande dépassé.
11  *      *      *      Délai d'attente de la demande dépassé.
12  226 ms 103 ms  75 ms  be102.rbx-g2-nc5.fr.eu [94.23.122.214]
13  *      *      *      Délai d'attente de la demande dépassé.
14  *      *      *      Délai d'attente de la demande dépassé.
15  *      *      *      Délai d'attente de la demande dépassé.
16  90 ms   83 ms  70 ms  ns3009290.ip-188-165-246.eu [188.165.246.136]
17  90 ms   98 ms  82 ms  ip130.ip-188-165-51.eu [188.165.51.130]

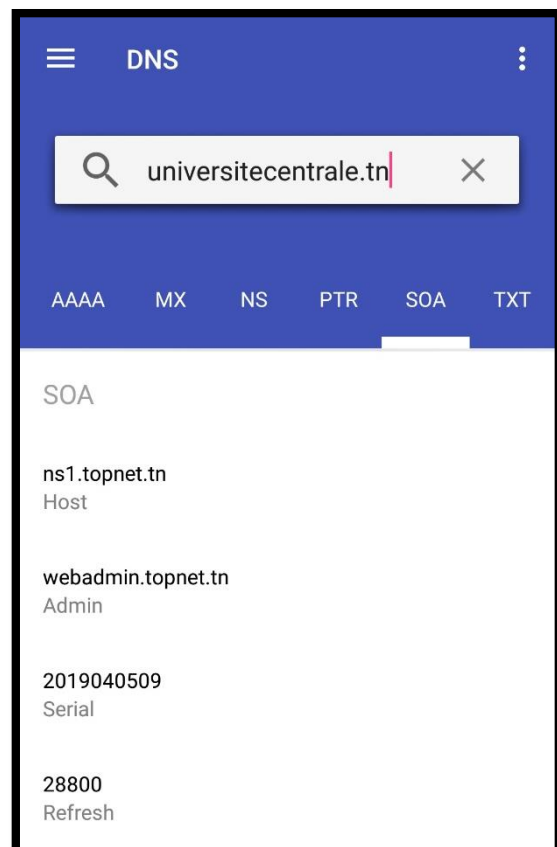
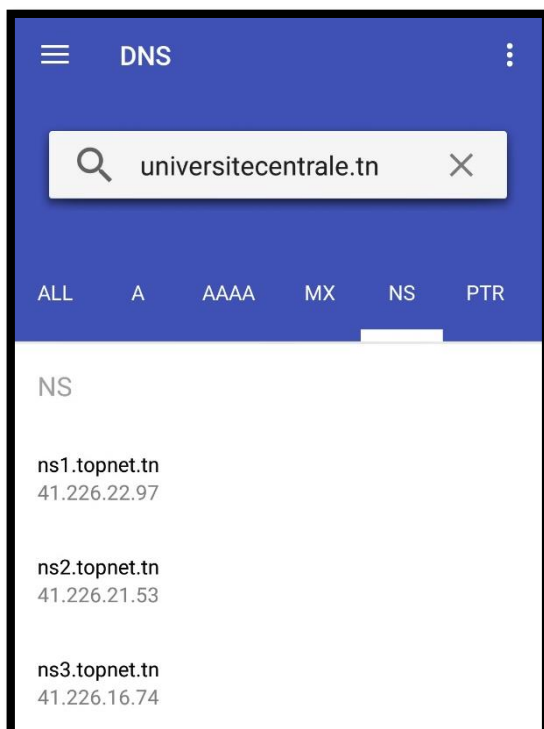
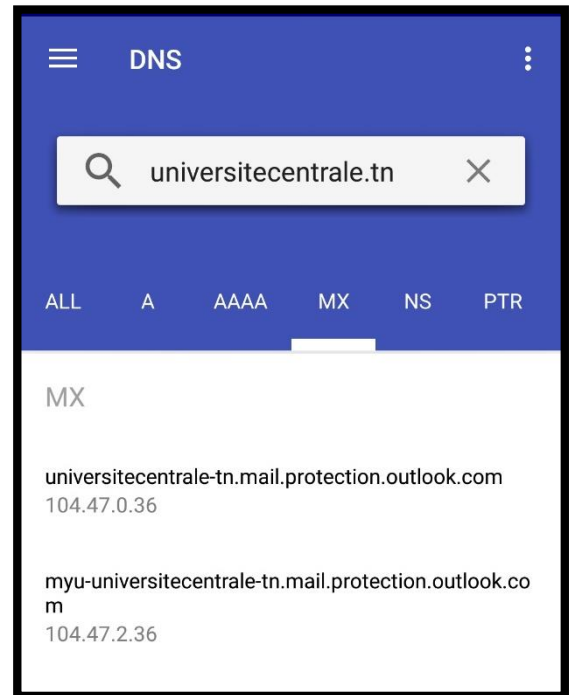
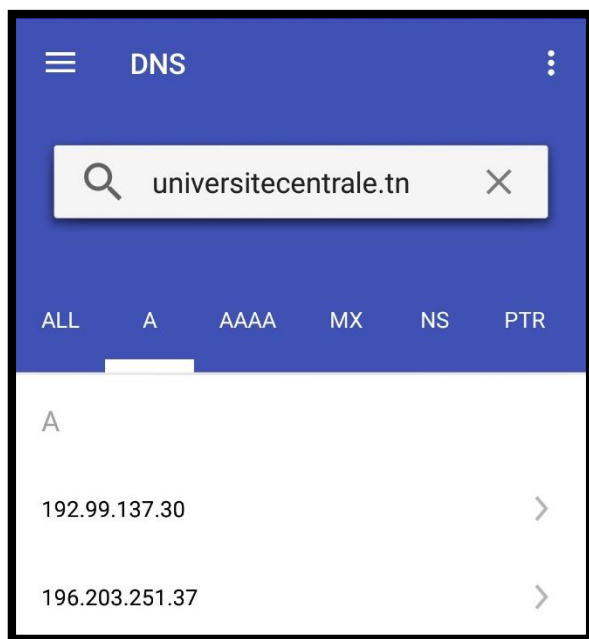
Itinéraire déterminé.
```

Nous avons atteint notre cible en 9 sauts.

## Commande nslookup

En tentant nslookup sur [universitecentrale.net](http://universitecentrale.net) je n'ai pas obtenu de résultats. Cependant j'ai essayé avec [universitecentrale.tn](http://universitecentrale.tn) et voici les résultats.

J'ai effectué cette commande depuis mon téléphone avec l'application « [Network Tools](#) ».



Voici les explications des différents enregistrements DNS.

Enregistrement [SOA](#) → [Start of Authority](#). C'est le serveur de nom du domaine. La différence avec l'enregistrement [NS](#) c'est qu'il fournit certaines informations supplémentaires dont l'adresse mail du contact technique (lorsqu'il y en a).

Enregistrement [NS](#) → [Name Server](#). Il indique quel serveur DNS fait autorité pour un domaine donné.

Enregistrement [A](#) → enregistrement de base. Pour un nom de de domaine donné, le DNS retourne l'adresse IP d'un serveur.

Enregistrement [PTR](#) → [Pointer Record](#). Il relie une adresse IP à un nom d'hôte. Un enregistrement PTR est parfois aussi appelé Reverse DNS Record.

Enregistrement [CNAME](#) → enregistrement de noms canoniques. Contrairement aux enregistrements A, ils ne peuvent pas être nus (c'est-à-dire qu'il doit y avoir [www](#). devant eux pour que l'URL résolve correctement). L'enregistrement CNAME indique que le nom de domaine indique que le nom de domaine est un alias d'un autre nom de domaine canonique.

Il est souvent utilisé pour rediriger une partie de son site Web vers un lien externe. Par exemple, si vous voulez créer un site eCommerce à côté de votre site Web existant, un enregistrement CNAM serait le moyen le plus simple de les relier.

Enregistrement [MX](#) → [Mail eXchanger](#). Il est utilisé pour diriger les emails envoyés aux adresses personnalisées associées à un nom de domaine. Il peut exister plusieurs MX par domaine afin de fournir, en cas de panne, une redondance des serveurs de messagerie. Pour cela, l'enregistrement MX permet de définir une priorité entre les différents enregistrements.

Enregistrement [SRV](#) → Permet de définir un serveur spécifique pour une application / un service. Cet enregistrement est notamment utilisé pour la répartition de charge.

## B. Recherche des personnes

1<sup>ère</sup> solution → <https://www.whitepages.com/>

Ce site ne fonctionne que sur le territoire américain.

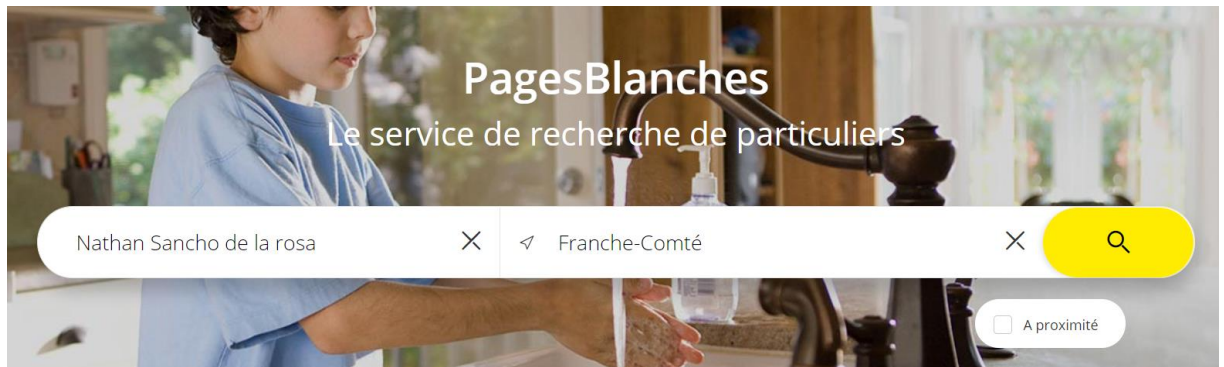
Dans mon exemple je cherche Brady Ellison (grand archer américain) et je trouve son domicile.

The screenshot shows the Whitepages search interface. At the top, there are tabs for PERSON, PHONE, REVERSE ADDRESS, and BUSINESS. The search bar contains "Brady Ellison" and a location field with "City, State or ZIP". Below the search bar, the results for "Brady Ellison" are displayed. On the left, there is a sidebar with "eviction reports." and a "Learn More" button. The main content area shows "Brady Lee Ellison" with "AGE 30s" and "Chula Vista, CA". It also lists "OTHER LOCATIONS" (Claypool, AZ; Payson, AZ; Glendale, AZ) and "FAMILY" members (Alfred Nathan Ellison, Samantha R Novak, Toja Ellison). A "View Details" button is present. At the bottom, there is a link to "Show all locations and family".

The screenshot shows the profile page for "Brady Lee Ellison". It includes a profile picture, the name "Brady Lee Ellison", and "Age 30s". There is a "Monitor" toggle switch set to "OFF". Below this, the "CURRENT ADDRESSES" section shows a home icon, the address "2134 Stellar Way Unit 2", and "Chula Vista CA 91915-2843". A map is displayed below the address, showing the location with a yellow pin. The map has "Map" and "Satellite" tabs, and a "HIDE MAP" link with an upward arrow.

2<sup>ème</sup> solution → <https://www.pagesjaunes.fr/pagesblanches>

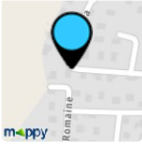
Ce site fonctionne sur des personnes vivant en France. Je tente par exemple sur mon camarade Nathan qui habite la région Franche-comté.



Je trouve son adresse ainsi que son numéro de téléphone

**Nathan Sancho de la rosa à Franche-Comté**  
2 résultats approchés

[Liste](#) [Carte](#) Pertinence ▼



**Sancho de la Rosa Patrice**  
16 r Jura, 25600 VIEUX CHARMONT

[Itinéraire](#) [Plan](#) [Afficher le n°](#)

Tél : 03 81 25 60 00

## C. Trace des emails

En ouvrant **eMailtrackerPro** je clique sur **Trace address** puis entre mon adresse mail.

Visualware eMailTrackerPro Trial (day 8 of 15)

[Configure](#) | [Help](#) | [About](#)

### eMailTrackerPro by Visualware

I Want To: \_\_\_\_\_

☐ Trace an email I have received

A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP ([more info](#)).

☒ Look up network responsible for an email address

An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

Enter Details: \_\_\_\_\_

Email address:

Dans l'encadré en bas on remarque qu'un traceroute est effectué et que le serveur mail est atteint en 14 sauts. Un point géographique est placé sur la France, il est très précis car il pointe sur la ville où se trouve mon école.

Dans l'encadré à droite nous avons un petit résumé de l'adresse IP du serveur ainsi que les services tournant sur cette machine.

The trace is complete, the information found is displayed on the right

#### Email Summary

Email Address: [nicolas.soares@utt.fr](mailto:nicolas.soares@utt.fr)  
IP: 194.214.201.9  
Location: France  
Abuse Address: [CerT@UTT.Besnet.fr](mailto:CerT@UTT.Besnet.fr)

System Information:

- The system is running a mail server (ESMTP.com) on port 25. This means that this system can be used to send email.
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

Network Whois  
Domain Whois

#	Hop	Hop IP	Hop Name	Location
1		192.168.43.1		
2		10.89.0.1		
3		192.168.253.30		
4		192.168.255.30		
5		194.149.164.92		(France)
6		194.149.166.117		(France)
7		80.249.209.251	amix-6b-1.routers.proxad.net	(Netherlands)
8		80.249.210.137		(Jordan)
9		62.40.98.129	ae9-mx1.lon.uk.giant.net	(United Kingdom)
10		62.40.98.57	ae6-mx1.lon2.uk.giant.net	(United Kingdom)
11		62.40.98.179	ae5-mx1.par.fr.giant.net	(United Kingdom)
12		83.97.89.10	renater-ias-renater-gw.par.fr.giant.net	(United Kingdom)
13		193.51.180.135		(France)
14		194.214.201.9	mx1-2.relay.renater.fr	(France)

Cependant ce qui est de la connexion à un compte email j'ai rencontré différents problèmes. Malgré des recherches internet ainsi que tentatives

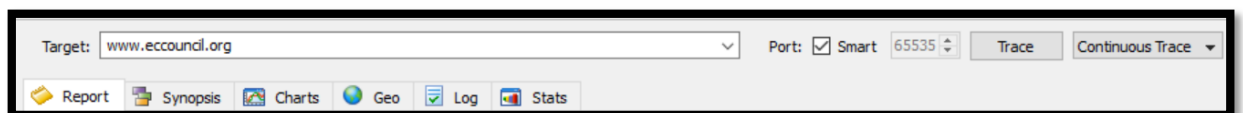
avec différents compte mails (outlook, gmail, @utt.fr pour mon adresse étudiante) rien ne change, le serveur le serveur refuse toute connexion et considère [eMailtrackerPro](#) comme logiciel pas assez sécurisé.

## D. Trace route du réseau

Lors de l'utilisation de [Path Analyzer Pro](#) j'ai rencontré certains problèmes. Après de nombreuses recherches sur internet, les solutions les plus appropriées sont de [désactiver le firewall Windows](#) (commande ci-dessous) et lancer Path Analyzer en [tant qu'administrateur](#).

```
C:\WINDOWS\system32>netsh advfirewall set allprofiles state off
Ok.
```

Pour lancer une trace il suffit de préciser la cible (URL ou adresse IP) puis de sélectionner « continuous Trace ».



Cependant une erreur persiste malgré la cible et les différentes configurations que j'ai pu tester. Je ne reçois aucun paquet de réponses après le 1<sup>er</sup> Time To Live.

Hop	IP Address	Hostname	ASN	Network Name	% Loss	Min Latency	Latency	Avg Latency	Max Latency	Std Dev
No reply packets received after TTL 1. You may try changing settings										

Dans l'onglet [Synopsis](#) nous retrouvons tout de même des informations importantes telles que les différents enregistrements DNS de la cible et le réseau auquel appartient la cible.

Report Synopsis Charts Geo Log Stats

### DNS

Multiple DNS address records were found for the hostname **www.eccouncil.org**. All the records will be listed below, but the first record (**104.18.20.251**) will be used for the analysis.

**Forward DNS (A-records)** 104.18.20.251  
[104.18.21.251](#)

**Reverse DNS (PTR-record)** www.eccouncil.org

### ROUTING

The IP address **104.18.20.251** is part of the network prefix **104.18.16.0/20** whose origin autonomous system is **13335**.

### REGISTRIES

The organization name on file at the registrar for this IP is **Cloudflare, Inc.** and the organization associated with the originating autonomous system is **Cloudflare, Inc..**

### INTERCEPT

The best point of lawful intercept is within the facilities of **Cloudflare, Inc..**

Nous retrouvons également d'autres informations dans les onglets de [log](#) et de [stats](#).

Report Synopsis Charts Geo Log Stats

### Current Trace Log

Using device eth0, 192.168.1.7  
 LFT trace started at 25-Oct-20 18:43:38 Paris, Madrid  
 SENT ICMP TTL=1  
 SENT ICMP TTL=2  
 SENT ICMP TTL=3  
 SENT ICMP TTL=4  
 SENT ICMP TTL=5  
 TTL 0 timed out, (resending)  
 SENT ICMP TTL=1  
 TTL 1 timed out, (resending)  
 SENT ICMP TTL=2  
 TTL 2 timed out, (resending)  
 SENT ICMP TTL=3

### Session Log

Using device eth0, 192.168.1.7  
 LFT trace started at 25-Oct-20 18:42:36 Paris, Madrid  
 SENT ICMP TTL=1  
 SENT ICMP TTL=2  
 SENT ICMP TTL=3  
 SENT ICMP TTL=4  
 SENT ICMP TTL=5  
 TTL 0 timed out, (resending)  
 SENT ICMP TTL=1  
 TTL 1 timed out, (resending)  
 SENT ICMP TTL=2  
 TTL 2 timed out, (resending)  
 SENT ICMP TTL=3  
 TTL 3 timed out, (resending)



Report Synopsis Charts Geo Log Stats							
Vital Statistics							
Source	Target	Protocol	Distance	Avg Latency	Trace Began	Trace Ended	Filters
192.168.1.7 (eth0: LAPTOP-OKP8A0QO.Home)	104.18.20.251	ICMP	1		25-Oct-20 18:43:38 ...	25-Oct-20 18:43:38 ...	1
192.168.1.7 (eth0: LAPTOP-OKP8A0QO.Home)	104.18.20.251	ICMP	1		25-Oct-20 18:43:29 ...	25-Oct-20 18:43:38 ...	1
Session Statistics							
Source	Target	Protocol	Distance	Avg Latency	Trace Began	Trace Ended	Filters
192.168.1.7 (eth0: LAPTOP-OKP8A0QO.Home)	104.18.20.251	ICMP	1		25-Oct-20 18:43:29 ...	25-Oct-20 18:43:38 ...	1
192.168.1.7 (eth0: LAPTOP-OKP8A0QO.Home)	196.203.251.37	ICMP	1		25-Oct-20 18:41:59 ...	25-Oct-20 18:42:45 ...	1
192.168.1.7 (eth0: LAPTOP-OKP8A0QO.Home)	104.18.20.251	ICMP	1		25-Oct-20 18:41:45 ...	25-Oct-20 18:41:54 ...	1
192.168.1.7 (eth0: LAPTOP-OKP8A0QO.Home)	196.203.251.37	ICMP	1		25-Oct-20 18:40:32 ...	25-Oct-20 18:40:41 ...	1
192.168.1.7 (eth0: LAPTOP-OKP8A0QO.Home)	104.18.20.251	ICMP	1		25-Oct-20 18:36:48 ...	25-Oct-20 18:36:57 ...	1
192.168.1.7 (eth0: LAPTOP-OKP8A0QO.Home)	104.18.20.251	ICMP	1		25-Oct-20 18:13:34 ...	25-Oct-20 18:13:44 ...	1
192.168.1.7 (eth0: LAPTOP-OKP8A0QO.Home)	104.18.20.251	ICMP	1		25-Oct-20 18:12:41 ...	25-Oct-20 18:12:50 ...	1

## E. Analyse du nom de domaine et de l'adresse IP

En démarrant [SmartWhois](#) un petit tutoriel nous explique les deux modes de fonctionnement du logiciel.

### Getting Started

#### Démarrer

L'utilisation de SmartWhois est facile ! Pour faire une requête d'adresse IP ou de domaine, entrez-la dans la zone de texte et cliquez " Comme IP / Nom d'hôte " :

**Auto Detect** **Enter**

As IP address / Hostname Shift+Ctrl+Enter

As Domain Ctrl+Enter

As IP / Hostname and Domain Shift+Alt+Enter

Custom Query ...

Pour faire une requête d'un nom de domaine, entrez-la dans la zone de texte et cliquez " Comme domaine "

**Auto Detect** **Enter**

As IP address / Hostname Shift+Ctrl+Enter

As Domain Ctrl+Enter


As IP / Hostname and Domain Shift+Alt+Enter


Custom Query ...


SmartWhois se connectera à une des bases de données mondiales Internet, puis affichera les informations que vous recherchez. Pour des informations détaillées sur les caractéristiques du programme, veuillez vous référer au [fichier d'aide](#).

Dans les résultats pour [www.eccouncil.org](http://www.eccouncil.org), nous retrouvons l'adresse IP de la cible, ensuite les informations sont malheureusement masquées.


**eccouncil.org**

 [eccouncil.org](http://eccouncil.org)


 104.18.20.251




Statutory Masking Enabled  
Statutory Masking Enabled  
Statutory Masking Enabled  
Statutory Masking Enabled




Statutory Masking Enabled  
Statutory Masking Enabled  
Statutory Masking Enabled  
Statutory Masking Enabled



HENRY.NS.CLOUDFLARE.COM  
ZELDA.NS.CLOUDFLARE.COM

 Alexa Traffic Rank : 24 017



Created: 2001-12-14T10:13:06Z  
Updated: 2018-02-03T02:39:19Z  
Expires: 2023-12-14T10:13:06Z  
Source: whois.networksolutions.com

Nous pouvons tout de même observer les enregistrements DNS et les dates importantes au niveau des certificats (le 1<sup>er</sup> ainsi que les certificats en cours).

Les résultats de [www.certifiedhacker.com](http://www.certifiedhacker.com) sont eux plus intéressants car les informations ont été laissées publiques.

IP, host or domain:  Query

**Results** × **certifiedhacker.com**

- certifiedhacker.com
- eccouncil.org

[certifiedhacker.com](http://certifiedhacker.com)

162.241.216.11

PERFECT PRIVACY, LLC  
5335 Gate Parkway care of Network Solutions PO Box 459  
Jacksonville  
FL  
32256  
United States  
Phone: +1.5707088780  
[v42h79ap9jx@networksolutionsprivateregistration.com](mailto:v42h79ap9jx@networksolutionsprivateregistration.com)

PERFECT PRIVACY, LLC  
5335 Gate Parkway care of Network Solutions PO Box 459  
Jacksonville  
FL  
32256  
United States  
Phone: +1.5707088780  
[v42h79ap9jx@networksolutionsprivateregistration.com](mailto:v42h79ap9jx@networksolutionsprivateregistration.com)

PERFECT PRIVACY, LLC  
5335 Gate Parkway care of Network Solutions PO Box 459  
Jacksonville  
FL  
32256  
United States  
Phone: +1.5707088780  
[v42h79ap9jx@networksolutionsprivateregistration.com](mailto:v42h79ap9jx@networksolutionsprivateregistration.com)

PERFECT PRIVACY, LLC  
5335 Gate Parkway care of Network Solutions PO Box 459  
Jacksonville  
FL  
32256  
United States  
Phone: +1.5707088780  
[v42h79ap9jx@networksolutionsprivateregistration.com](mailto:v42h79ap9jx@networksolutionsprivateregistration.com)

NS1.BLUEHOST.COM  
NS2.BLUEHOST.COM

Alexa Traffic Rank : 3 102 289

Created: 2002-07-30T00:32:00Z  
Updated: 2020-08-22T08:32:48Z  
Expires: 2021-07-30T00:32:00Z  
Source: whois.networksolutions.com

Completed at 25/10/2020 20:34:01  
Processing time: 2,94 seconds  
[View source](#)

## F. Extraction des données d'une entreprise

Une fois webextractor lancé quelques étapes sont à effectuer :

- Nommer le projet
- Préciser le lien du site web où l'on veut extraire les données
- Cocher les différentes données que l'on veut extraire.

The screenshot shows the 'Session' dialog box in WebExtractor. The 'General' tab is active. The 'Session name' field is set to 'TP\_foot\_printing'. The 'Start URL' is 'www.eccouncil.org'. The 'Depth' is set to 100. The 'Data source' is set to 'Site'. The 'Extraction data' section is checked for 'Emails', 'Phones', and 'Faxes'. The 'Custom data expressions' section is empty. The 'Start!' button is highlighted.

Session

General

Session name: TP\_foot\_printing

Group:

Timeline: New Session

Data source: ☒ Site ☐ Search Engines ☐ Url List

Start URL: www.eccouncil.org

Depth: 100

☒ Positive ☒ Negative

☐ Fixed number of pages

Advanced

Cookie: Capture

Initial referer:

Extraction data

☐ Custom data

☐ URLs ☐ Proxy

☐ Domains

☐ Meta Tags

☒ Emails Filter

☒ Phones Filter

☐ Faxes

Custom data expressions: not complete

Custom Data Editor + Data1

Begins with: \*

Contains: \*

Ends with: \*

☒ Remove HTML Tags

Help Start! Close

Voici une capture de la session en cours, nous pouvons voir depuis quand la session est lancée, quels sont les URLs visités ainsi que la quantité de données téléchargé.

Web Data Extractor Pro 3.10. Trial Version. You are on day 2 of your 15 day evaluation period.

new session edit session start pause stop 0 B/s options

Process log \*Results Bad URLs (2) Stored Sessions

URL	Title	State	Size	Downloaded
https://www.eccouncil.org/about	About Us   EC-Council	Parse		165 251
https://ciso.eccouncil.org/ciso-events	CISO Events - EC-Council	Parse		94 429
https://iclass.eccouncil.org/masterclass-penetration-tester...	EC-Council iClass   Online ECSA   ...	Download		507 115
https://iclass.eccouncil.org/masterclass-certified-ethical-h...	EC-Council iClass   Online Certified...	Download		475 045
https://iclass.eccouncil.org/masterclass-soc-analyst-progr...	EC-Council iClass   Online CSA   C...	Download		275 567
https://iclass.eccouncil.org/masterclass-network-defender...	EC-Council iClass   Online CND   ...	Download		231 024
https://www.eccouncil.org/ece-endorsed-events	Endorsed Events   Cyber Security ...	Download		287 820
https://www.eccouncil.org/bug-bounty	EC-Council Bug Bounty Program   ...	Download		146 456
https://www.eccouncil.org/ec-council-global-awards	EC-Council Global Awards   EC-Co...	Download		294 762
https://www.eccouncil.org/accreditations	Accreditations   EC-Council	Download		145 224
https://www.eccouncil.org/xmlrpc.php		Request (2%)		
https://www.eccouncil.org/xmlrpc.php?rsd		Request (2%)		
https://www.eccouncil.org/about/accredited-training-cent...		Request (14%)		
https://www.eccouncil.org/partner-with-us		Request (6%)		
https://try.eccouncil.org/vapt-track		Request (5%)		
https://blog.eccouncil.org/3-secure-methodologies-to-cre...		Request		
https://blog.eccouncil.org/ec-council-partners-with-aisa-to...		Request		
https://blog.eccouncil.org/martin-andreev-cyber-security-e...		Request		
https://blog.eccouncil.org/3-secure-methodologies-to-cre...		Request		

Processing time: 00:00:30.688 Sites processed: 46 / 185 Downloaded: 14 356 KB Avg. Speed: 487 KB/s

Dans l'onglet résultats nous pouvons consulter les données qui nous intéressent et qui ont été extraites.

Web Data Extractor Pro 3.10. Trial Version. You are on day 2 of your 15 day evaluation period.

new session edit session start pause stop 355 KB/s options

Process log \*Results Bad URLs (297) Stored Sessions

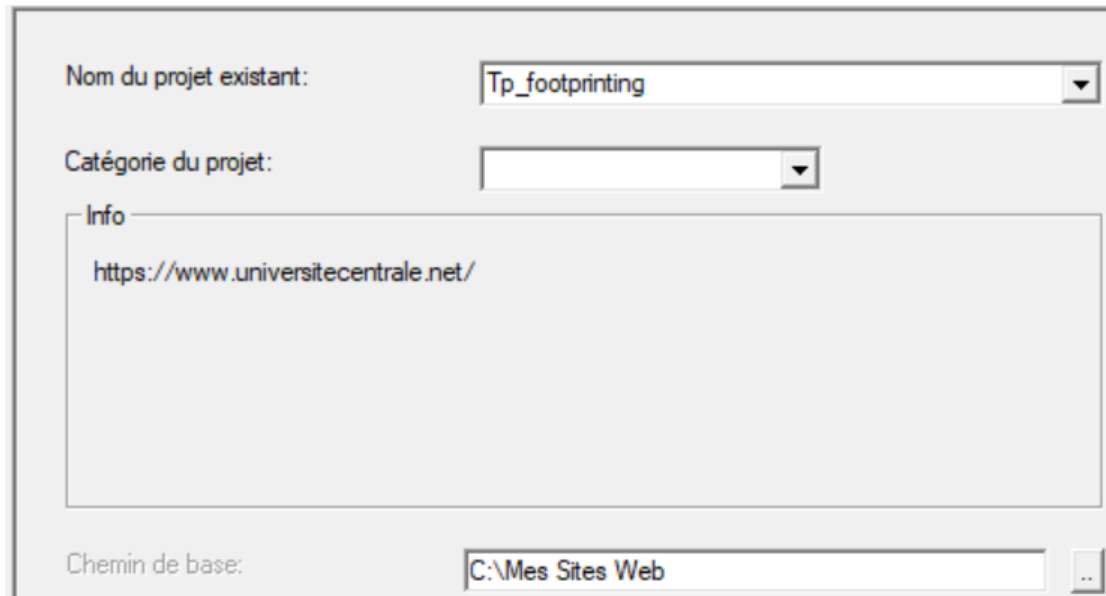
Email (30) Phone (4342)

Email	Name	Url	Title	Host
practicals@eccoun...	practicals	https://www.eccouncil.org/programs...	EC-Council Certified Securit...	eccouncil.org
lpt@eccouncil.org	lpt	https://www.eccouncil.org/programs...	Advanced Penetration Tes...	eccouncil.org
Steve.graham@ec...	Steve.graham	https://www.eccouncil.org/govemme...	Government & Military   Cyb...	eccouncil.org
aspensupport@ecc...	aspensupport	https://aspensupport.eccouncil.org/...	Find Training   ASPEN	aspensupport.eccouncil.org
feedback@eccoun...	feedback	https://www.eccouncil.org/programs...	Penetration Testing   EC-C...	eccouncil.org
aspensupport@ecc...	aspensupport	https://aspensupport.eccouncil.org/...	Home   ASPEN	aspensupport.eccouncil.org
feedback@eccoun...	feedback	https://www.eccouncil.org/programs...	Certified Ethical Hacker   C...	eccouncil.org
mycontributions@e...	mycontributions	https://www.eccouncil.org/become-a...	Become an EC-Council Su...	eccouncil.org
cast@eccouncil.org	cast	https://www.eccouncil.org/programs...	Advanced Network Defens...	eccouncil.org
membersupport@e...	membersupport	https://www.eccouncil.org/partner-wi...	Partner with us   Accredited...	eccouncil.org
legal@eccouncil.org	legal	https://www.eccouncil.org/terms-of-u...	Terms of Use   EC-Council	eccouncil.org
info@cisomag.com	info	https://cisomag.eccouncil.org/?utm_...	Cybersecurity Magazine   C...	cisomag.eccouncil...
cciso@eccouncil.org	cciso	https://ciso.eccouncil.org/cciso-certif...	CISO FAQ - EC-Council	ciso.eccouncil.org
cehapp@eccouncil...	cehapp	https://cert.eccouncil.org/faq.html	FAQ   CERT	cert.eccouncil.org
certmanager@ecc...	certmanager	https://cert.eccouncil.org/application...	Home   CERT	cert.eccouncil.org
certmanager@ecc...	certmanager	https://cert.eccouncil.org/application...		cert.eccouncil.org
certmanager@ecc...	certmanager	https://cert.eccouncil.org/application...		cert.eccouncil.org

Processing time: 00:02:23.974 Sites processed: 527 / 670 Downloaded: 42 421 KB Avg. Speed: 296 KB/s

## G. Copie des sites web

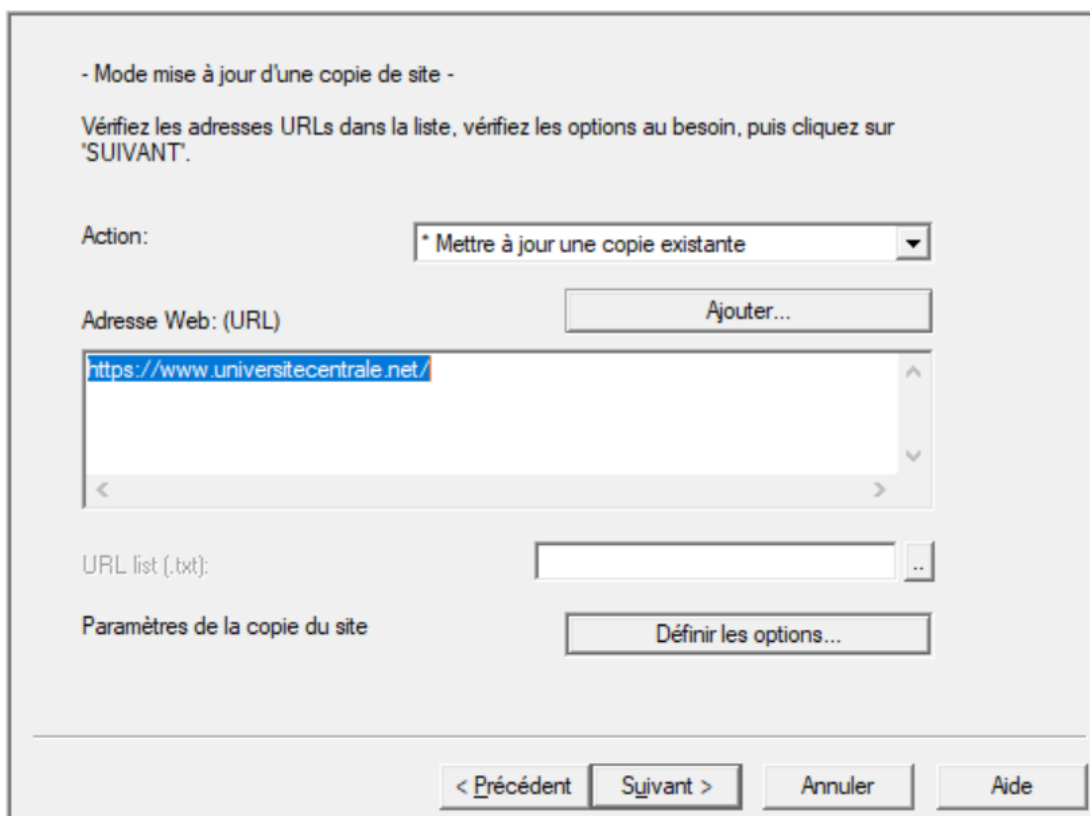
Pour démarrer une copie, il suffit de nommer notre projet et préciser le chemin où sera placée la copie du site.



A screenshot of a software dialog box for copying a website. It contains the following fields and controls:

- Nom du projet existant:** A dropdown menu with the text "Tp\_footprinting".
- Catégorie du projet:** An empty dropdown menu.
- Info:** A text area containing the URL "https://www.universitecentrale.net/".
- Chemin de base:** A text field containing "C:\Mes Sites Web" with a browse button (three dots) to its right.

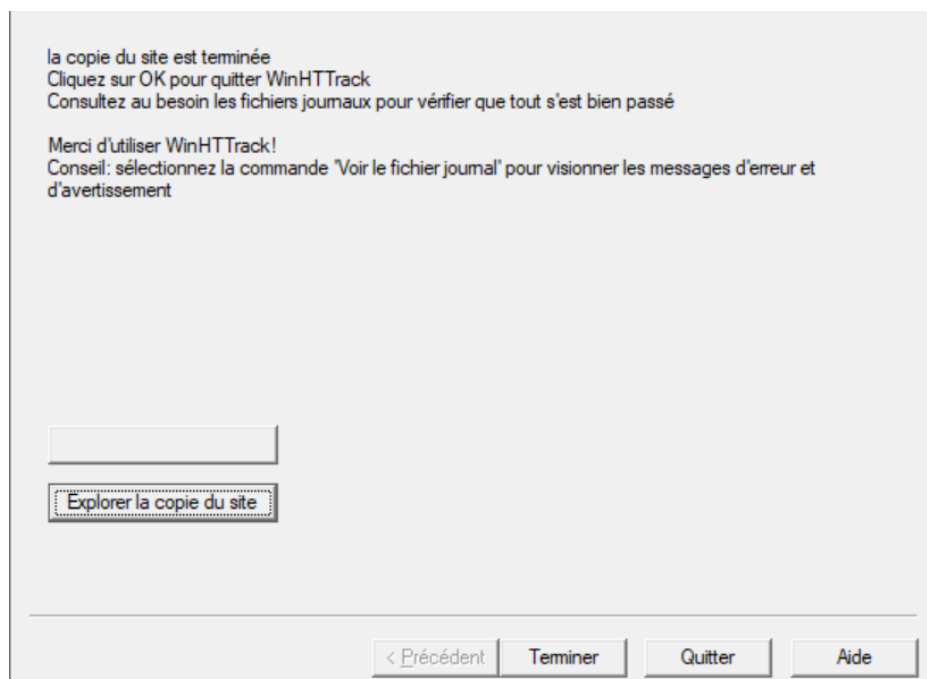
Ensuite il suffit de préciser le lien du site que nous voulons copier et lancer la réplication.



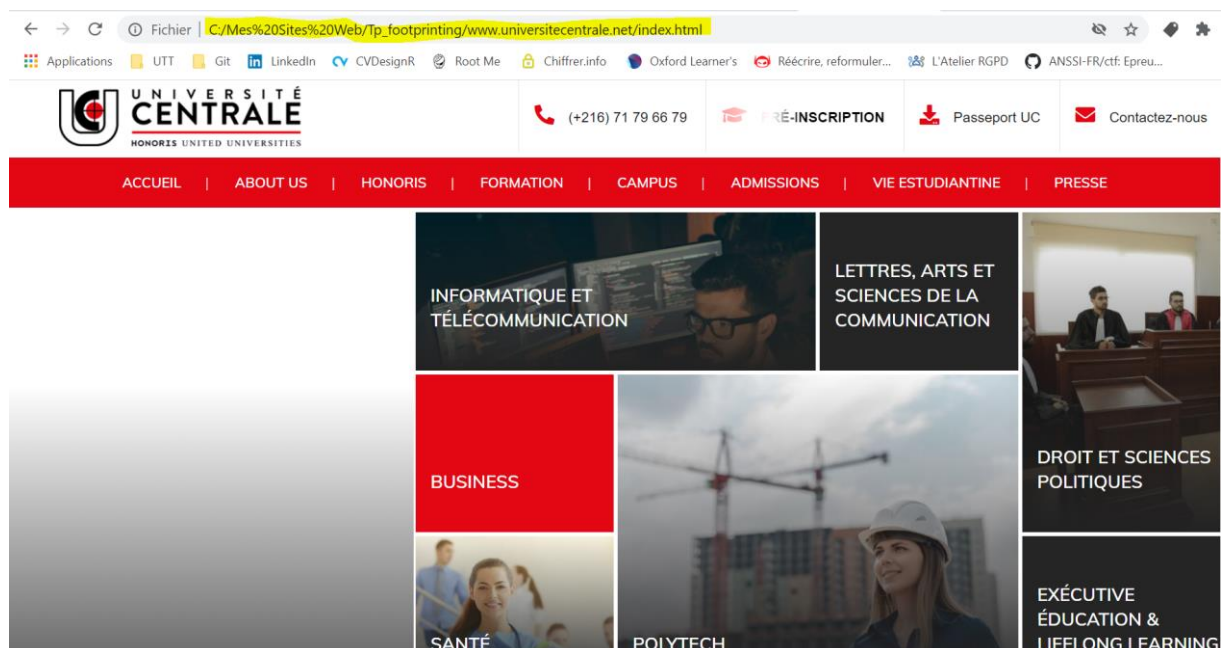
A screenshot of a software dialog box for configuring website copy options. It contains the following fields and controls:

- Mode mise à jour d'une copie de site -**: A title bar or section header.
- Vérifiez les adresses URLs dans la liste, vérifiez les options au besoin, puis cliquez sur 'SUIVANT'.**: Instructional text.
- Action:** A dropdown menu with the selected option "Mettre à jour une copie existante".
- Adresse Web: (URL)**: A text field containing "https://www.universitecentrale.net/" with a blue selection highlight. To its right is an "Ajouter..." button.
- URL list (.txt):** A text field with a browse button (three dots) to its right.
- Paramètres de la copie du site**: A button labeled "Définir les options...".
- Footer buttons:** Four buttons at the bottom: "< Précédent", "Suivant >", "Annuler", and "Aide".

Après un temps de travail plus ou moins long suivant le site choisi, un journal d'erreur est rédigé afin de voir si certaines actions n'ont pas abouti.

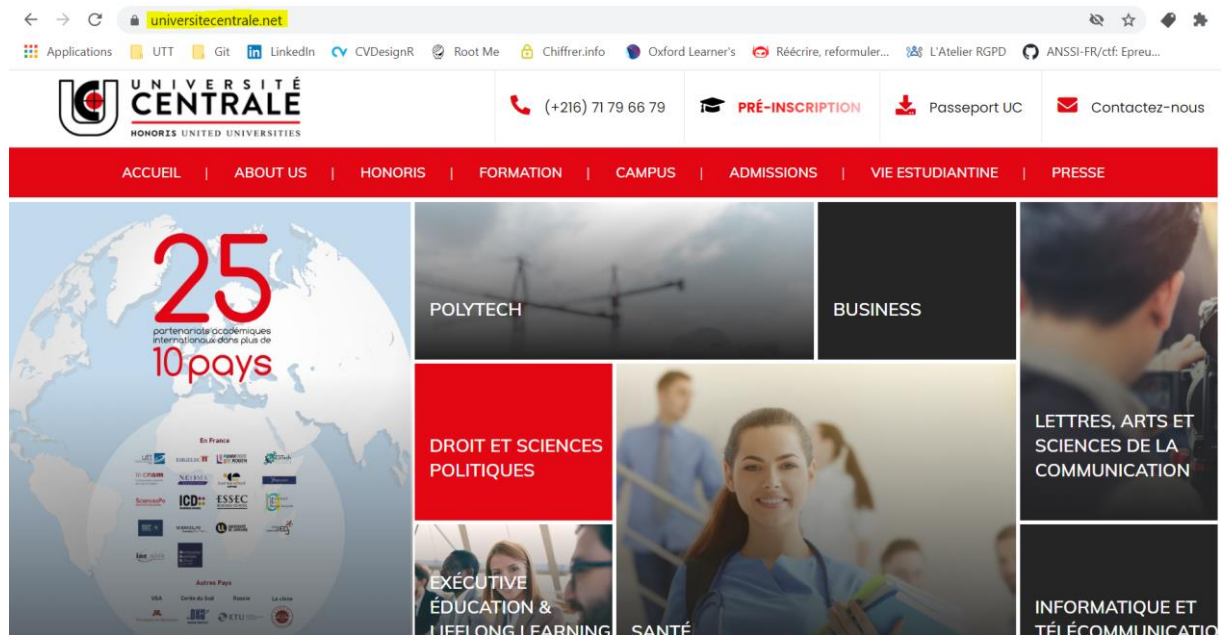


Nous pouvons également parcourir le site qui a été copié. Comme on peut le lire dans l'URL, c'est bien une copie du site de l'université centrale que je parcours depuis un fichier local de mon PC.

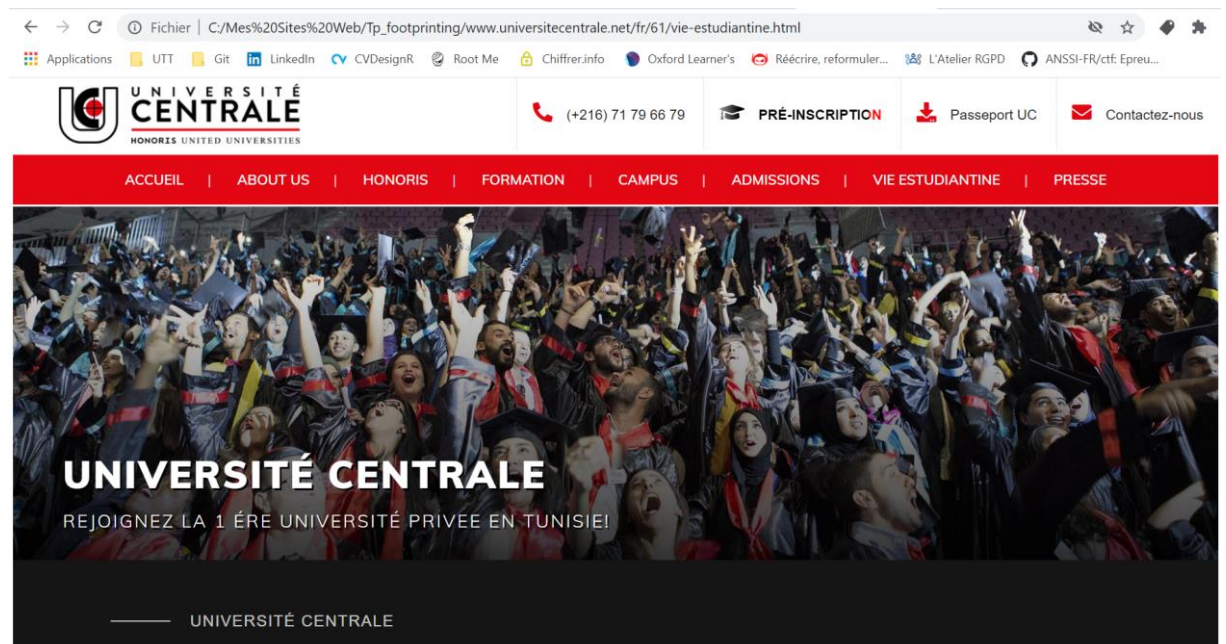




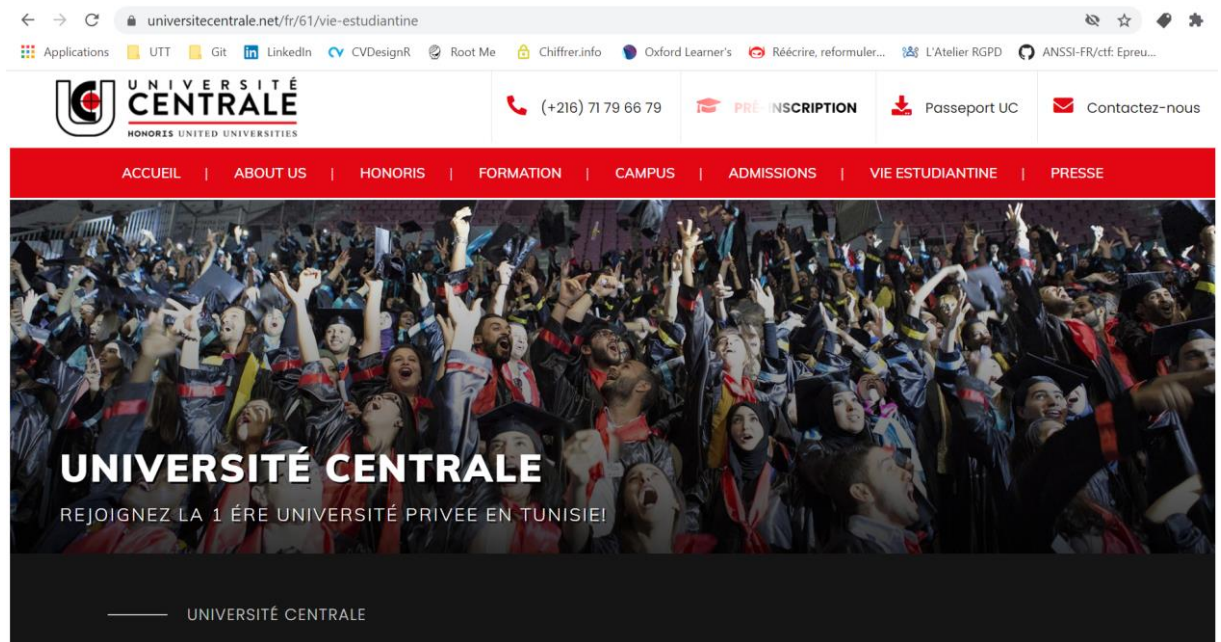
Mis à part l'encadré à gauche qui dans ma copie reste gris, la réplique est bluffante.



Voici un exemple avec une autre page, on peut voir que le site est identique.





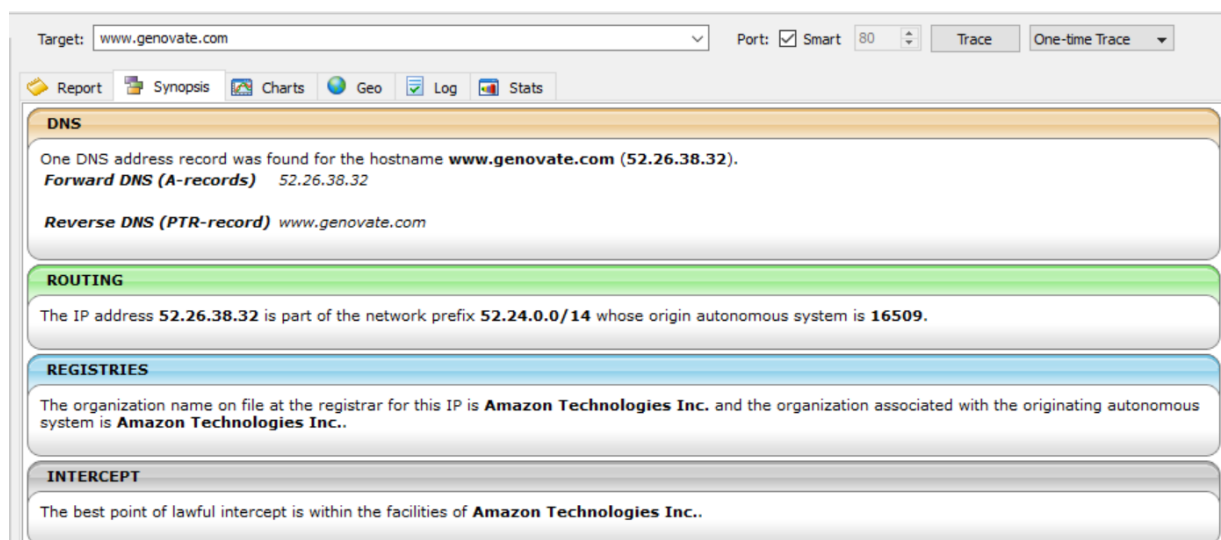


## H. Exercice reconnaissance

Le nom de l'entreprise est : [Genova](#)

Avec une simple recherche google, le site est : <https://www.genovate.com/>

Je utiliser un [terminal de commande](#) ou bien le logiciel [Path Anlayzer Pro](#) afin de connaître l'adresse IP de la cible et les différents enregistrements DNS.



Ensuite pour les informations sur l'entreprise (contact, certificat...) j'utilise simplement [google](#) et aussi [SmartWhois](#)

## CONTACT INFO

Our customer support team is happy to help you with any questions that you may have, or to help you initiate a file for DNA testing.

Toll Free Tel: [1-855-976-1058](tel:1-855-976-1058)  
Toll Free Fax: [1-888-655-8877](tel:1-888-655-8877)  
Customer Support: [support@genovate.com](mailto:support@genovate.com)  
Technical Support: [lab@genovate.com](mailto:lab@genovate.com)  
Accounts: [accounts@genovate.com](mailto:accounts@genovate.com)

IP, host or domain:  Query

Results

certifiedhacker.com

eccouncil.org

**genovate.com**

www.genovate.com

52.26.38.32

genovate.com

[genovate.com](#)

52.26.38.32

PERFECT PRIVACY, LLC  
5335 Gate Parkway care of Network Solutions PO Box 459  
Jacksonville  
FL  
32256  
United States  
Phone: +1.5707088780  
[vc8847n54n4@networksolutionsprivateregistration.com](mailto:vc8847n54n4@networksolutionsprivateregistration.com)

PERFECT PRIVACY, LLC  
5335 Gate Parkway care of Network Solutions PO Box 459  
Jacksonville  
FL  
32256  
United States  
Phone: +1.5707088780  
[vc8847n54n4@networksolutionsprivateregistration.com](mailto:vc8847n54n4@networksolutionsprivateregistration.com)

PERFECT PRIVACY, LLC  
5335 Gate Parkway care of Network Solutions PO Box 459  
Jacksonville  
FL  
32256  
United States  
Phone: +1.5707088780  
[vc8847n54n4@networksolutionsprivateregistration.com](mailto:vc8847n54n4@networksolutionsprivateregistration.com)

NS17.WORLDDNIC.COM  
NS18.WORLDDNIC.COM



Alexa Traffic Rank : 3 827 318



Created: 1998-12-30T05:00:00Z

Updated: 2017-12-22T23:12:43Z

Expires: 2022-12-30T05:00:00Z

Source: whois.networksolutions.com

Completed at 26/10/2020 13:46:22

Processing time: 9,20 seconds

[View source](#)

Il existe beaucoup d'autres logiciels qui permettent d'effectuer ces recherches mais une commande est également très intéressante (nmap). C'est ce que nous allons voir dans le TP suivant de scanning.