

# COURS OSINT

23.01.2023



**PROGRAMME**

## Description du Cours

Ce cours d'Open Source Intelligence (OSINT) fournira aux étudiants la capacité à rassembler des informations sur des personnes, des groupes ou des entreprises à partir de sources diverses. Il fournira une série de compétences allant de la préservation de l'anonymat à la création de fausses identités en ligne, en passant par la compréhension du besoin, la collecte, le traitement, la diffusion et la capitalisation de l'information. Les étudiants se verront présenter les méthodologies et les outils les plus utilisés en renseignement cyber de sources ouvertes, au travers de modules théoriques, techniques et d'ateliers pratiques.

### OBJECTIFS DES ATELIERS

- Donner à l'étudiant les compétences nécessaires pour réaliser des techniques d'investigation tout en restant anonyme ;
- Permettre à l'étudiant de se familiariser avec des outils spécialisés et d'en comprendre les résultats ;
- Présenter des ressources en ligne peu connues ;
- Formaliser les résultats d'une investigation.

## Admission

Semestre A2S1, A2S2

Pré-requis : Aucun

## Règles de savoir vivre





















L'assiduité au cours est la base d'un apprentissage réussi.

Si vous ne pouvez pas assister au cours pour des raisons personnelles ou liées à votre alternance, il est de bon ton de prévenir à l'avance l'enseignant.

Un registre des présents sera tenu sur toute la durée du cours.

## Compétences à acquérir en 2ème Année

 Table

| Aa Code_compétence...        | Description   | Ref_RNCP_Competence   | Ref_RNCP_Activite   | Ref_RNCP_Block   | Année | Syllabus  |
|------------------------------|---|---|---|--|-------|---|
| <a href="#">SEC-OSI_2_01</a> | Employer des opérateurs de recherche avancés  |  <a href="#">RNCP_CO13</a> |  <a href="#">RNCP_AC04</a> |  <a href="#">RNCP_BLK03</a> | 2     |  <a href="#">OSINT</a> |
| <a href="#">SEC-OSI_2_02</a> | Concevoir une investigation numérique à base de source ouverte ciblant un acteur ou une organisation. |  <a href="#">RNCP_CO04</a> |  <a href="#">RNCP_AC02</a> |  <a href="#">RNCP_BLK01</a> | 2     |  <a href="#">OSINT</a> |
| <a href="#">SEC-OSI_2_03</a> | Évaluer les différents outils en source ouverte à des fins d'investigations numériques.               |  <a href="#">RNCP_CO07</a> |  <a href="#">RNCP_AC03</a> |  <a href="#">RNCP_BLK02</a> | 2     |  <a href="#">OSINT</a> |
| <a href="#">SEC-OSI_2_04</a> | Formaliser les résultats d'une investigation  |  <a href="#">RNCP_CO03</a> |  <a href="#">RNCP_AC01</a> |  <a href="#">RNCP_BLK01</a> | 2     |  <a href="#">OSINT</a> |
| <a href="#">SEC-OSI_2_05</a> | Restituer oralement les résultats d'une investigation   |  <a href="#">RNCP_CO03</a> |  <a href="#">RNCP_AC01</a> |  <a href="#">RNCP_BLK01</a> | 2     |  <a href="#">OSINT</a> |

# Agenda du cours

Table

| Aa Intitulé           | Type            | Semestre | Promo | Date                        | Matière |
|-----------------------|-----------------|----------|-------|-----------------------------|---------|
| OSINT n°1             | Cours Magistral | A2S1     | 2024  | 23 janvier 2023 9:30-11:30  | ! OSINT |
| Exercices d'OSINT n°1 | TP              | A2S1     | 2024  | 23 janvier 2023 12:30-17:30 | ! OSINT |
| OSINT n°2             | Cours Magistral | A2S1     | 2024  | 24 janvier 2023 9:30-11:30  | ! OSINT |
| Exercices d'OSINT n°2 | TP              | A2S1     | 2024  | 24 janvier 2023 12:30-17:30 | ! OSINT |
| OSINT n°3             | Cours Magistral | A2S1     | 2024  | 25 janvier 2023 10:30-11:30 | ! OSINT |
| Exercices d'OSINT n°3 | TP              | A2S1     | 2024  | 25 janvier 2023 12:30-17:30 | ! OSINT |
| OSINT n 4             | Cours Magistral | A2S1     | 2024  | 26 janvier 2023 9:30-11:30  | ! OSINT |
| Exercices d'OSINT n 4 | TP              | A2S1     | 2024  | 26 janvier 2023 12:30-17:30 | ! OSINT |
| OSINT Projet          | Suivi           | A2S2     | 2024  | 6 mars 2023 17:00-17:30     | ! OSINT |
| OSINT Devoir          | Devoir          | A2S2     | 2024  | 16 avril 2023 23:59         | ! OSINT |
| OSINT Soutenance 1    | Soutenance      | A2S2     | 2024  | 17 avril 2023 9:30-11:30    | ! OSINT |
| OSINT Soutenance 2    | Soutenance      | A2S2     | 2024  | 17 avril 2023 12:30-15:30   | ! OSINT |



## Évaluation

La session de cours de A2S1 sera évaluée par la réalisation de mini défis individuels. Les réponses seront transmises via un questionnaire interactif en ligne. Un temps imparti sera défini au début de chaque défi.

La session de cours de A2S2 sera évaluée par la réalisation d'un projet en groupe de 6-7 étudiants (même groupe que Forensic) donnant lieu au rendu d'un rapport et à une soutenance de projet 20 minutes (15 minutes de présentation, 5 minutes de questions).



## Notation

### Pondération

Mini défis (30%)

Rapport (40%)

Soutenance (30%)

### Échelle de notation

0 Compétence non constatée

1 Compétence non acquise

2 Compétence en cours  
d'acquisition

3 Compétence acquise

4 Maîtrise

5 Expertise

### Correspondance sur 20

0 devoir non rendu

1  $1 \leq \text{note} < 7.5$

2  $7.5 \leq \text{note} < 11.5$

3  $11.5 \leq \text{note} < 13.5$

4  $13.5 \leq \text{note} < 20$

5  $\text{note} \geq 20$

### Rendu des devoirs

Les mini défis de A2S1 seront à rendre sous la forme d'un questionnaire interactif en ligne.

Les rapports de A2S2 seront envoyés à l'adresse [pierre.blondel.ext@ecole2600.com](mailto:pierre.blondel.ext@ecole2600.com) par le chef de projet de chaque groupe au plus tard le 16 avril 2022 à 23h59.

La soutenance se déroulera le 17 avril 2022 et fera l'objet d'une présentation.

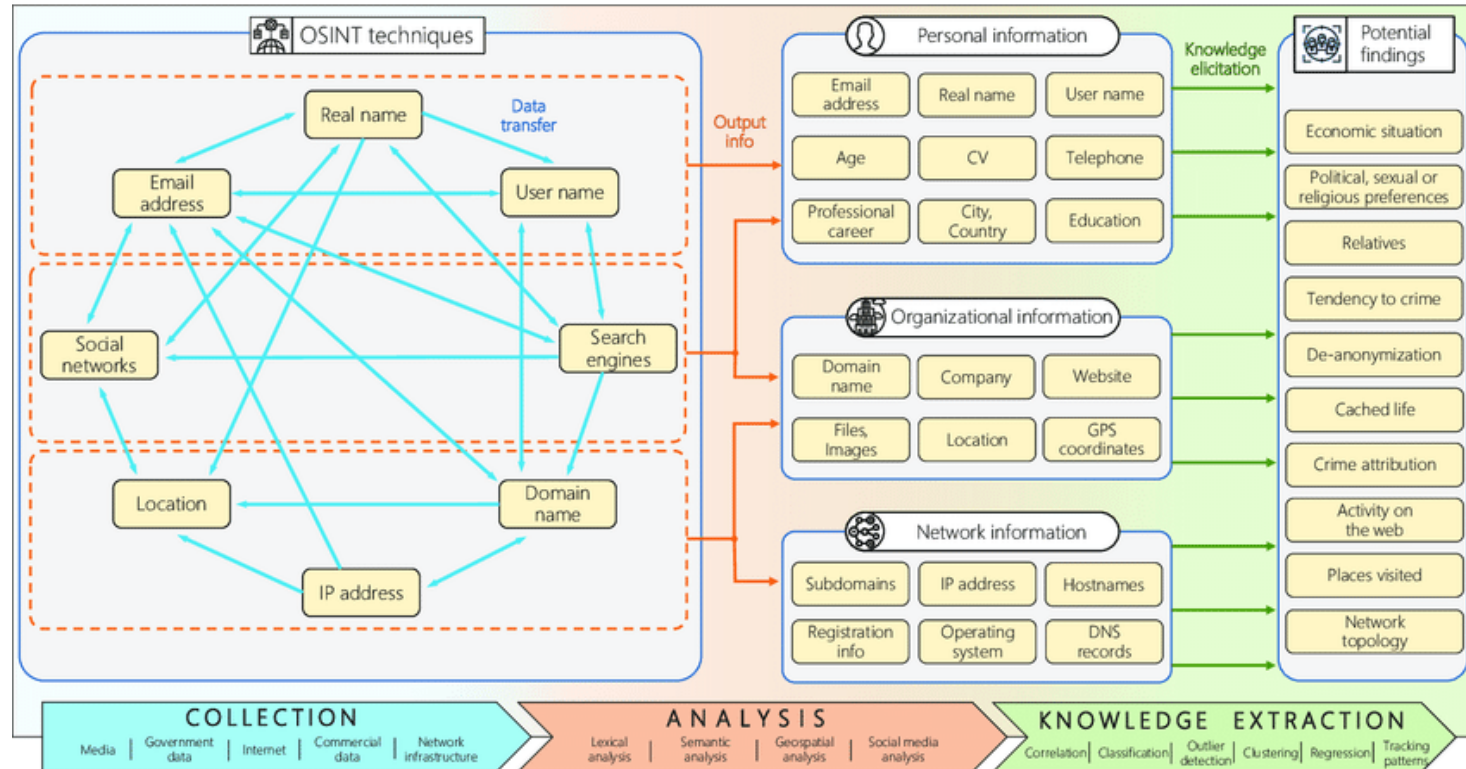
### Devoirs non rendus ou rendus en retard

Tout devoir non rendu se verra attribuer la note minimale (zéro).

Tout devoir rendu au-delà des délais impartis se verra sanctionné par une pénalité d'1 niveau dans l'échelle de notation avec pour minimal le niveau 1.

# MÉTHODOLOGIE

# Workflow

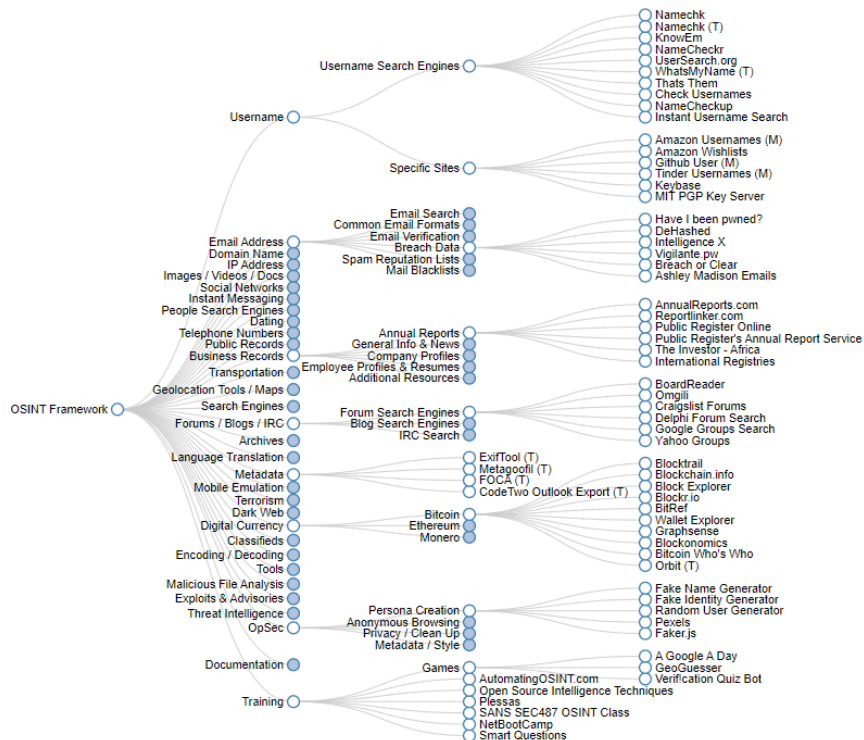




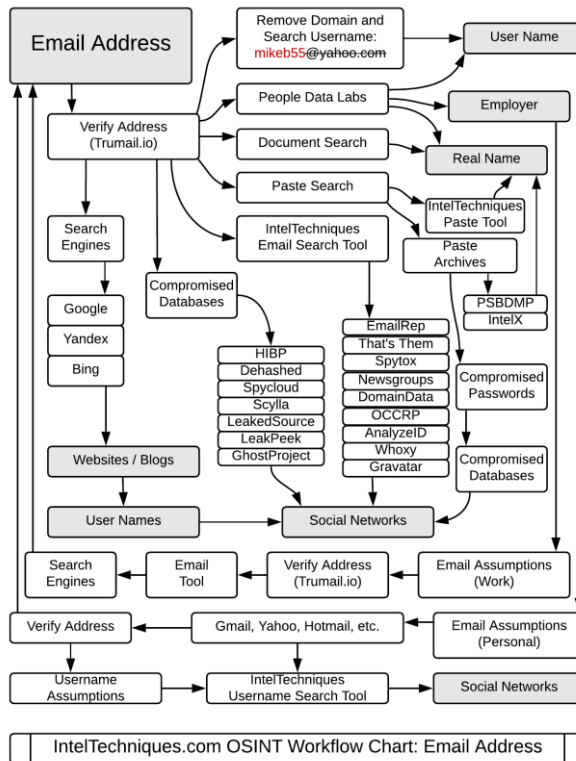
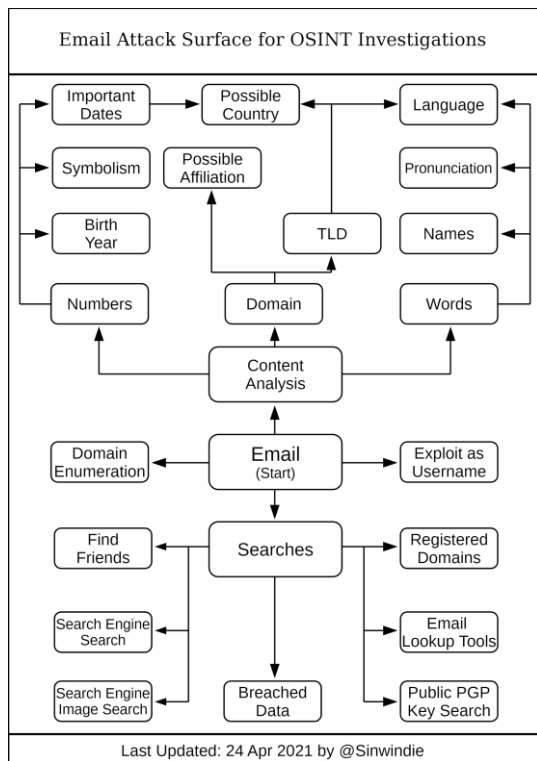
# Workflow

## OSINT Framework

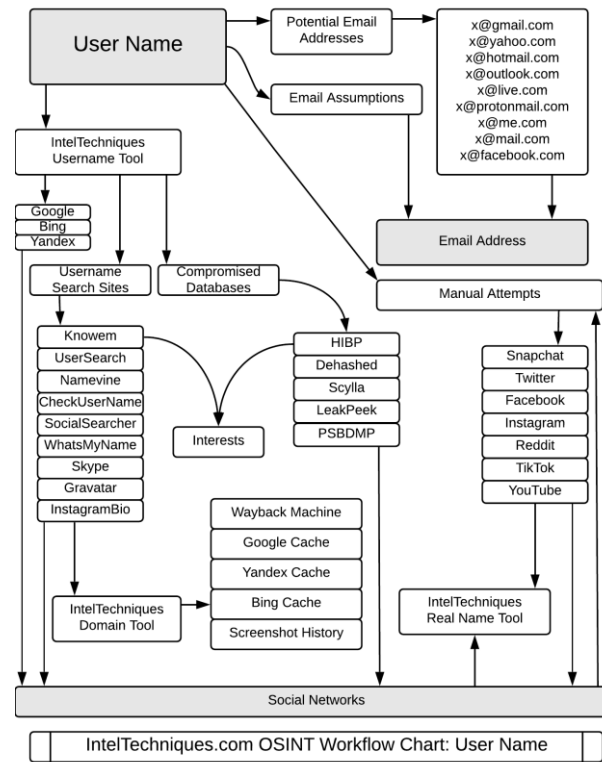
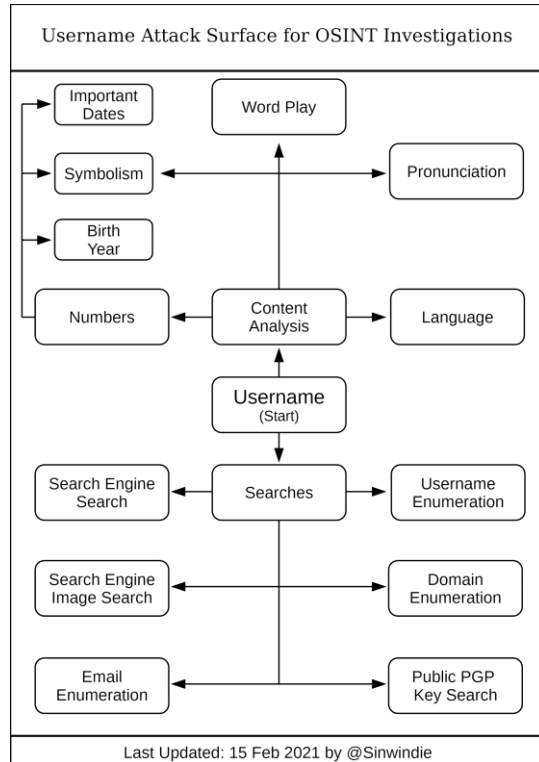
(T) - Indicates a link to a tool that must be installed and run locally  
(D) - Google Dork, for more information: [Google Hacking](#)  
(R) - Requires registration  
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually



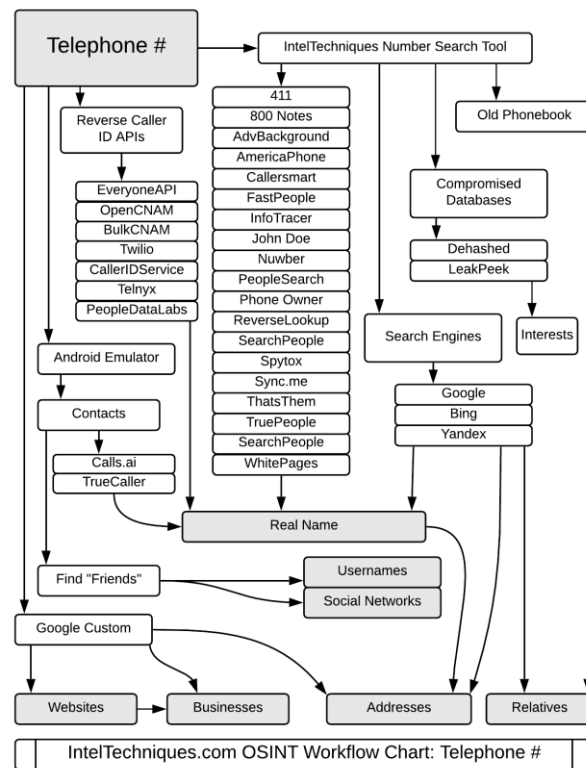
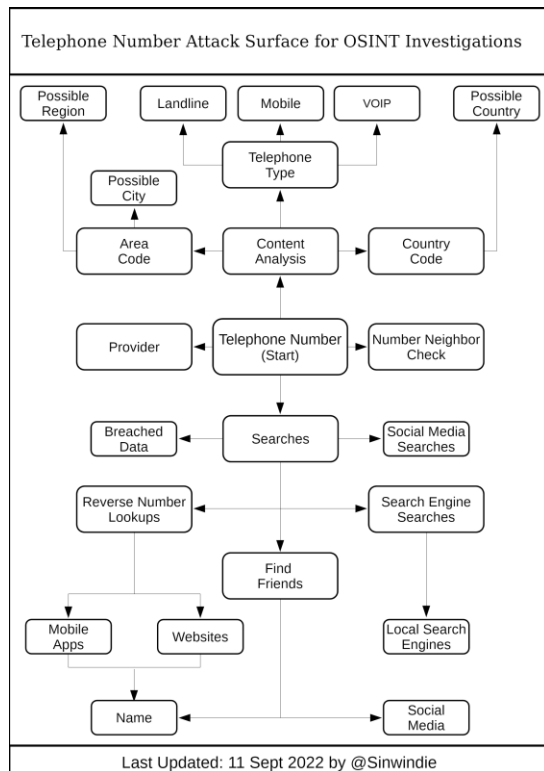
# Workflow (email)



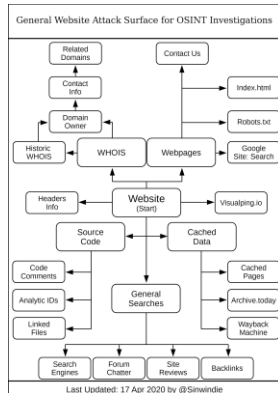
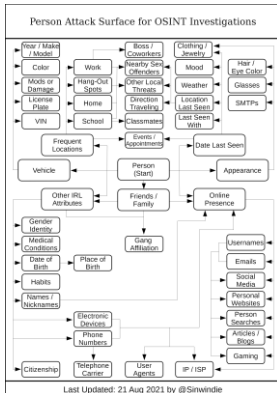
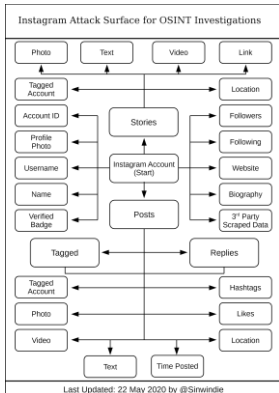
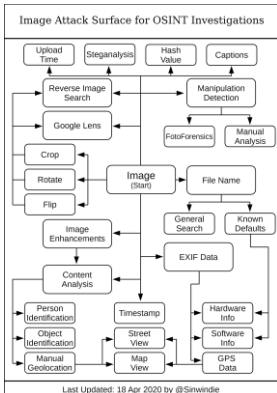
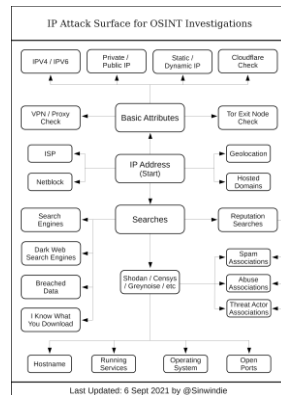
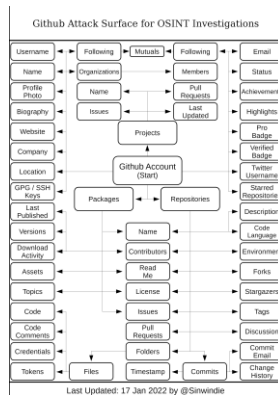
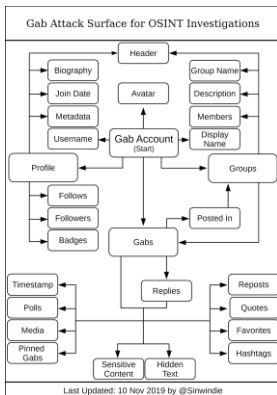
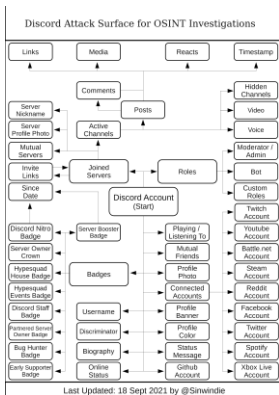
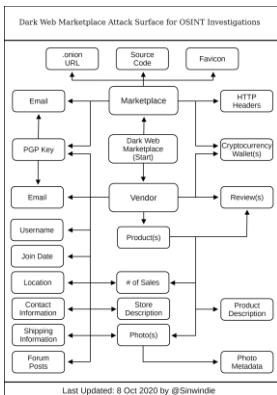
## Workflow (username)



# Workflow (numéro de téléphone)



## Workflow (...)



**MACHINE VIRTUELLE**

# Virtualisation



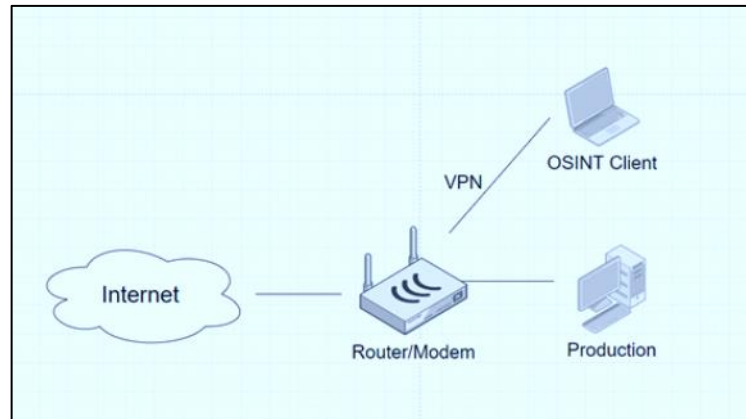
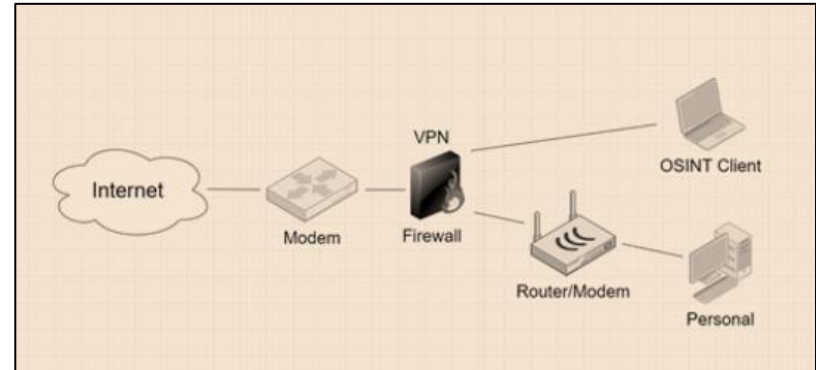
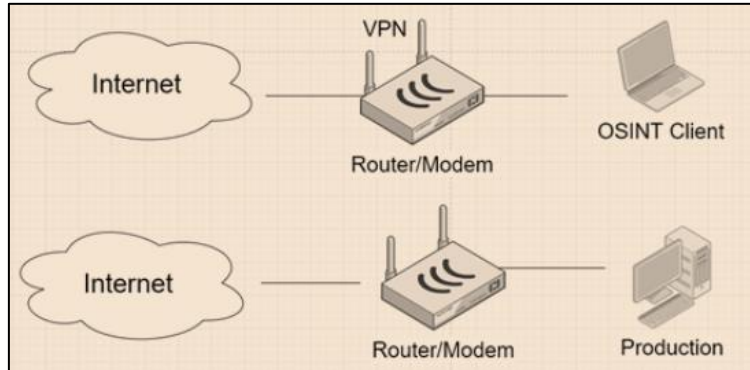
**VirtualBox**



**vmware®**



# Cloisonnement (réseaux)





# Distribution/OS



# Virtual Private Network (VPN)

 ProtonVPN

windscribe



# Virtual Private Server (VPS)



# Emulateur Android

Genymotion



developers 

# Navigateur

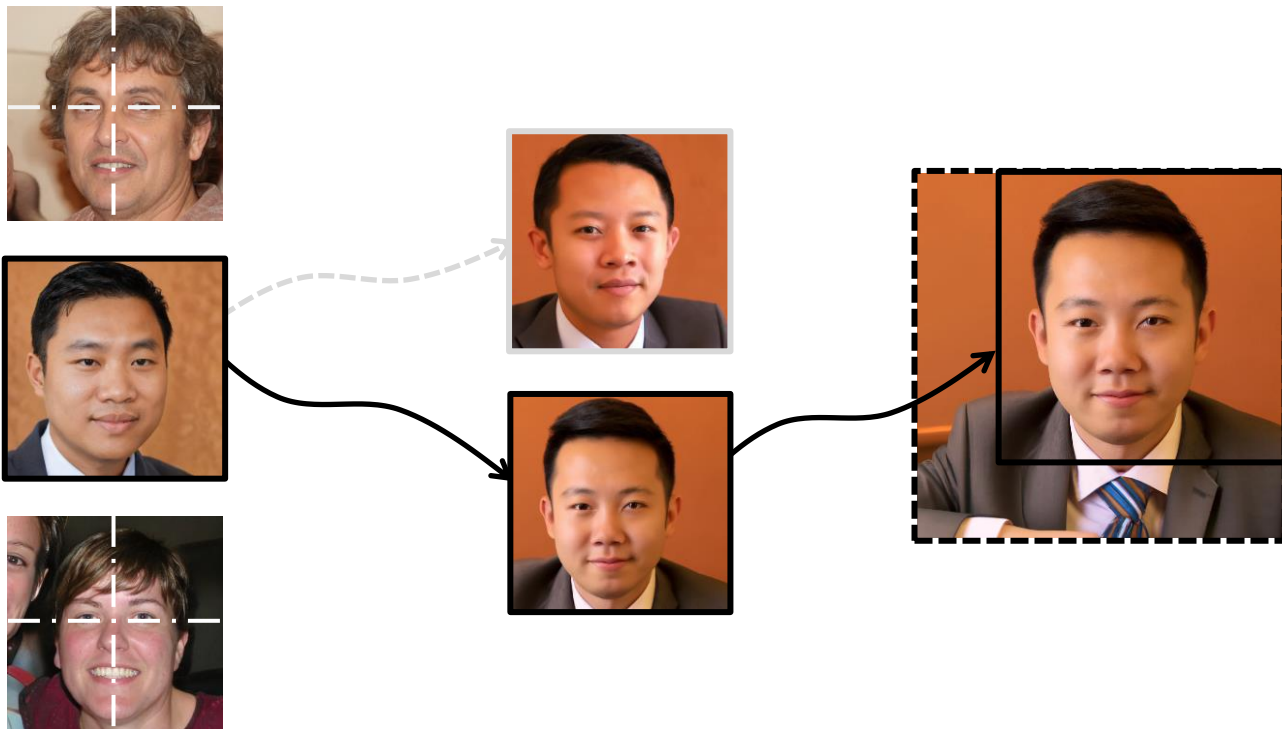


**SOCKPUPPET**

# AVATAR



# AVATAR





**OUTILS**

# MOTEURS DE RECHERCHE & DORKS

- `site: *.ecole2600.com`
- `site: *.ecole2600.*`
- `site: *.ecole2600.com -www`
- `inurl: ecole2600`
- `ip:106.26.02.201`
- `cache:ecole2600.com`
- `intitle:ecole2600`
- `site:onedrive.live.com ecole2600`
- `site:s3.amazonaws.com ecole2600`
- `site:drive.google.com ecole2600`
- `site:dl.dropbox.com ecole2600`



DuckDuckGo



...

# DEFI 3

(OSINT ON)

# Document

**Matériel :**



**Règles :**

- Retrouver le seul pdf indexé par Google issue du site web ecole2600.com;
- Page 5, retrouver nom du casque ainsi que son poids sans le câble au gramme près;
- Page 9 de ce pdf, retrouver la taille du moniteur secondaire derrière l'ordinateur portable;
- Page 12 de ce pdf, retrouver le nom et prénom de l'individu sur la photo, son compte LinkedIn, le nom de l'appareil photo, ainsi que l'objectif utilisé.
- Page 16, compléter cette ligne de code présente sur son moniteur : « filter-status-item-wrapper » : **[????]**, »
- Page 19 de ce pdf, que regarde l'homme en pull rouge ?
- Page 22 de ce pdf, quel est la marque de son second moniteur ?
- Page 24 de ce pdf, quel est la marque de la montre située sur le poignet gauche ?

**Durée :**

20 min

# DEFI 4

(OSINT ON)

# Document

**Matériel :**



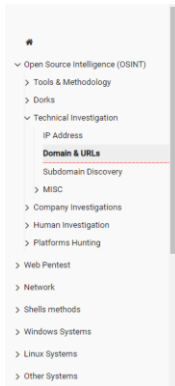
**Règles :**

- Retrouver le seul pdf indexé par Google issue du site web ecole2600.com;
- Page 5, retrouver nom du casque ainsi que son poids sans le câble au gramme près;
- Page 9 de ce pdf, retrouver la taille du moniteur secondaire derrière l'ordinateur portable;
- Page 12 de ce pdf, retrouver le nom et prénom de l'individu sur la photo, son compte LinkedIn, le nom de l'appareil photo, ainsi que l'objectif utilisé.
- Page 16, compléter cette ligne de code présente sur son moniteur : « filter-status-item-wrapper » : [????], »
- Page 19 de ce pdf, que regarde l'homme en pull rouge ?
- Page 22 de ce pdf, quel est la marque de son second moniteur ?
- Page 24 de ce pdf, quel est la marque de la montre située sur le poignet gauche ?

**Durée :**

45 min

# LISTES



## DOMAIN & URLS

### Getting Informations

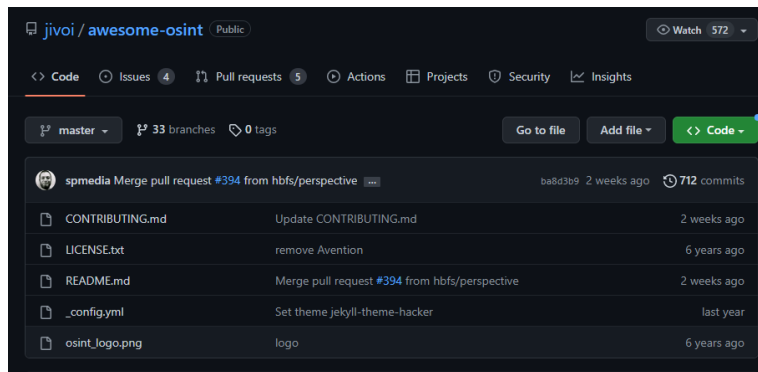
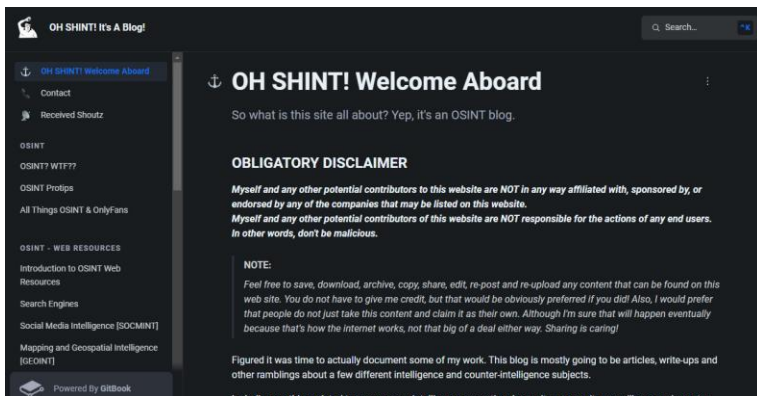
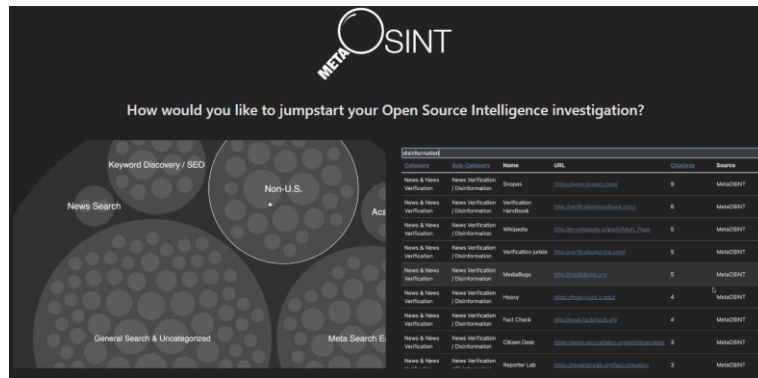
```
Get information on an IP
whois <IP>

# Get IP address associated to a domain
nslookup domain.fr
ping domain.fr

# Knockknock is a small automated script allowing you to find domain names
# For a registrant (person or company)
python3 k2.py -n company -d

# Many tools
https://intelix.io/

# Estimate the creation date of a website
http://carbondate.cs.odu.edu/
https://github.com/Lazza/Carbon14
```





- [github.com/OWASP/Amass](https://github.com/OWASP/Amass)
- [github.com/projectdiscovery/subfinder](https://github.com/projectdiscovery/subfinder)
- [github.com/laramies/theHarvester](https://github.com/laramies/theHarvester)
- [github.com/aboul3la/Sublist3r](https://github.com/aboul3la/Sublist3r)
- [github.com/thewhiteh4t/FinalRecon](https://github.com/thewhiteh4t/FinalRecon)
- [github.com/lanmaster53/recon-ng](https://github.com/lanmaster53/recon-ng)
- [github.com/darkoperator/dnsrecon](https://github.com/darkoperator/dnsrecon)
- [github.com/davidpepper/fierce-domain-scanner](https://github.com/davidpepper/fierce-domain-scanner)
- [github.com/darklotusdb/sd-goo](https://github.com/darklotusdb/sd-goo)
- [github.com/shmilylty/OneForAll](https://github.com/shmilylty/OneForAll)
- [github.com/infosec-au/altdns](https://github.com/infosec-au/altdns)
- [github.com/psjs97/GoogleEnum](https://github.com/psjs97/GoogleEnum)
- [github.com/screetsec/Sudomy](https://github.com/screetsec/Sudomy)
- [github.com/yunxu1/dnsuB](https://github.com/yunxu1/dnsuB)
- [github.com/Acmesec/Sylas](https://github.com/Acmesec/Sylas)
- [github.com/v4d1/Dome](https://github.com/v4d1/Dome)
- [github.com/Fadavvi/Sub-Drill](https://github.com/Fadavvi/Sub-Drill)
- [github.com/devanshbatham/Passivehunter](https://github.com/devanshbatham/Passivehunter)
- [github.com/oxPugazh/SubDomz](https://github.com/oxPugazh/SubDomz)
- ...







crt.sh Identity Search



[Group by Issuer](#)

Criteria Type: Identity Match: ILIKE Search: 'ecole2600.com'

| Certificates | crt.sh ID                  | Logged At  | Not Before | Not After  | Common Name            | Matching Identities    | Issuer Name                  |
|--------------|----------------------------|------------|------------|------------|------------------------|------------------------|------------------------------|
|              | <a href="#">8444907980</a> | 2023-01-19 | 2023-01-19 | 2023-04-19 | gf2rtfa.ecole2600.com  | gf2rtfa.ecole2600.com  | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8457244789</a> | 2023-01-12 | 2023-01-12 | 2023-04-12 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8398036571</a> | 2023-01-12 | 2023-01-12 | 2023-04-12 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8438347015</a> | 2023-01-10 | 2023-01-10 | 2023-04-10 | training.ecole2600.com | training.ecole2600.com | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8386663370</a> | 2023-01-10 | 2023-01-10 | 2023-04-10 | training.ecole2600.com | training.ecole2600.com | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8429093591</a> | 2023-01-09 | 2023-01-09 | 2023-04-09 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8401909134</a> | 2023-01-09 | 2023-01-09 | 2023-04-09 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8400792332</a> | 2023-01-06 | 2023-01-06 | 2023-04-06 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8357090481</a> | 2023-01-06 | 2023-01-06 | 2023-04-06 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8400772177</a> | 2023-01-06 | 2023-01-06 | 2023-04-06 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8357086167</a> | 2023-01-06 | 2023-01-06 | 2023-04-06 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8344017827</a> | 2023-01-01 | 2023-01-01 | 2023-04-01 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8334578165</a> | 2023-01-01 | 2023-01-01 | 2023-04-01 | lea.ecole2600.com      | lea.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8294410199</a> | 2022-12-26 | 2022-12-26 | 2023-03-26 | llc.ecole2600.com      | llc.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8290905159</a> | 2022-12-26 | 2022-12-26 | 2023-03-26 | llc.ecole2600.com      | llc.ecole2600.com      | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8231462070</a> | 2022-12-17 | 2022-12-17 | 2023-03-17 | r.ecole2600.com        | r.ecole2600.com        | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8223989331</a> | 2022-12-17 | 2022-12-17 | 2023-03-17 | r.ecole2600.com        | r.ecole2600.com        | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8173323075</a> | 2022-12-09 | 2022-12-09 | 2023-03-09 | portal.ecole2600.com   | portal.ecole2600.com   | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8157212805</a> | 2022-12-09 | 2022-12-09 | 2023-03-09 | portal.ecole2600.com   | portal.ecole2600.com   | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8162943701</a> | 2022-12-07 | 2022-12-07 | 2023-03-07 | opco.ecole2600.com     | opco.ecole2600.com     | C=US, O=Let's Encrypt, CN=R3 |
|              | <a href="#">8144742462</a> | 2022-12-07 | 2022-12-07 | 2023-03-07 | opco.ecole2600.com     | opco.ecole2600.com     | C=US, O=Let's Encrypt, CN=R3 |

# CERTIFICATE TRANSPARENCY

- [github.com/google/certificate-transparency-go](https://github.com/google/certificate-transparency-go)
- [github.com/google/certificate-transparency](https://github.com/google/certificate-transparency)
- [transparencyreport.google.com/https/certificates](https://transparencyreport.google.com/https/certificates)
- [github.com/lanrat/certgraph](https://github.com/lanrat/certgraph)
- [github.com/CaliDog/certstream-python](https://github.com/CaliDog/certstream-python)
- [crt.sh](https://crt.sh)
- [censys.io](https://censys.io)
- [developers.facebook.com/tools/ct](https://developers.facebook.com/tools/ct)
- [letsencrypt.org/docs/ct-logs](https://letsencrypt.org/docs/ct-logs)



ALIEN VAULT

Pulses

0

Passive DNS

123


URLs

1

Files

0

## Analysis Overview

|                |   |
|----------------|---|
| IP Address     | <a href="#">104.26.2.201</a> , <a href="#">104.26.3.201</a> , <a href="#">172.67.72.219</a>     |
| Location       |  United States |
| ASN            | AS13335 cloudflare  |
| Nameservers    | <a href="#">carla.ns.cloudflare.com.</a> , <a href="#">harvey.ns.cloudflare.com.</a>            |
| WHOIS          | Registrar: OVH, SAS, Creation Date: Mar 5, 2019   |
| Related Pulses | None  |
| Related Tags   | None  |

### Indicator Facts

Running webserver 22 subdomains Resolves to 3 IPs

**SPF record**

### External Resources

[Whois](#), [UrlVoid](#), [VirusTotal](#)

# TYPOSQUATTING






- [github.com/urbanadventurer/urlcrazy](https://github.com/urbanadventurer/urlcrazy)
- [github.com/elceef/dnstwist](https://github.com/elceef/dnstwist)
- [github.com/atenreiro/opensquat](https://github.com/atenreiro/opensquat)
- [github.com/monkeym4ster/DomainFuzz](https://github.com/monkeym4ster/DomainFuzz)
- [github.com/ail-project/ail-typo-squatting](https://github.com/ail-project/ail-typo-squatting)



ecole2600.com

Scan

Scanned 2076 permutations. Found 5 registered: [share it](#) or download as [CSV](#) [JSON](#)

| PERMUTATION   | IP ADDRESS  | NAME SERVER                       | MAIL SERVER                               |
|---|---|-----------------------------------|---|
| ecole2600.com <br>*original  | 104.26.2.201<br>2606:4700:20::681a:2c9<br>United States | carla.ns.cloudflare.com           | _dc-<br>mx.1b43e85d3fdc.ecole2600.co<br>m |
| ecole26oo.com <br>homoglyph  | 213.186.33.5<br>France                                  | dns101.ovh.net                    | mx3.mail.ovh.net                          |
| école2600.com <br>homoglyph  | 216.239.32.21<br>2001:4860:4802:32::15<br>Mexico        | ns-cloud-<br>b1.googledomains.com |   |
| ecole2.600.com <br>subdomain | 205.178.189.129<br>United States                        |                                   |   |
| ecole2600.eu <br>tld-swap    | 213.186.33.5<br>France                                  | dns102.ovh.net                    | mx3.mail.ovh.net                          |



identified: 283, checked: 283, resolved: 3

**Protect your business from phishing attacks and IP infringement!**

Subscribe and we'll alert you as soon as someone registers a domain similar to **ecole2600.com**.










[Subscribe Now!](#)

Free 28-day trials available and no credit card required!

Found (3)

Available (280)

[export csv](#)

| Domain                                  | IP Address / A record   | MX record? |   |
|---|---|------------|---|
| ecole2.600.com                          |  205.178.189.129 | ×          |   |
| école2600.com<br>(xn--cole2600-goa.com) |  216.239.32.21   | ×          |   |
| ecole2600.com                           |  172.67.72.219   | ✓          |   |

ghryj.eu

Help

Search

Share

Grid

Chat

10 / 97

Community Score

10 security vendors flagged this domain as malicious

ghryj.eu

command and control compromised websites unknown

DETECTION

DETAILS

RELATIONS

COMMUNITY

Categories

Forcepoint ThreatSeeker compromised websites

Sophos command and control

Comodo Valkyrie Verdict unknown

Webroot Phishing and Other Frauds

alphaMountain.ai Malicious

Last DNS Records

| Record type | TTL   | Value           |
|-------------|-------|-----------------|
| A           | 21600 | 5.255.88.84     |
| NS          | 21600 | dns4.regway.com |
| NS          | 21600 | dns3.regway.com |
| NS          | 21600 | dns2.regway.com |
| NS          | 21600 | dns1.regway.com |
| + SOA       | 7200  | dns1.regway.com |

Last HTTPS Certificate

JARM Fingerprint

26d26d16d26d26d22c26d26d26dfd9c9d14e4f4f67f94f0359f8b28f532

Chat

# NOMS DE DOMAINE DÉCENTRALISÉS (BNS)

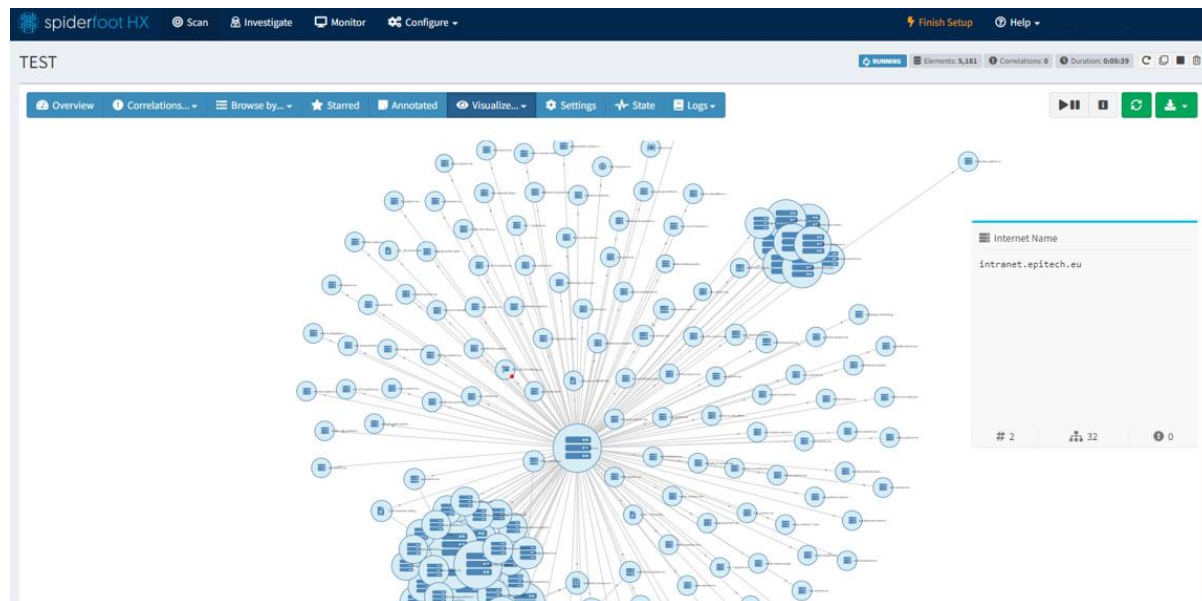




# AUTOMATISATION

# CERTSTREAM

```
[2023-01-08T13:08:48.828418] https://ct.googleapis.com/logs/argon2023/ - epitech.ronin.cat
[2023-01-08T14:29:01.548998] https://ct.googleapis.com/logs/xenon2023/ - epitech-startero1.sciado.fr
[2023-01-08T14:29:01.841826] https://ct.googleapis.com/logs/argon2023/ - epitech-startero1.sciado.fr
[2023-01-08T14:55:59.669347] https://oak.ct.letsencrypt.org/2023/ - epitech-startero2.sciado.fr
[2023-01-08T14:56:52.693587] https://ct.googleapis.com/logs/xenon2023/ - epitech-startero2.sciado.fr
[2023-01-08T14:57:06.837278] https://ct.googleapis.com/logs/argon2023/ - epitech-startero2.sciado.fr
[2023-01-08T21:57:10.519178] https://nessie2023.ct.digicert.com/log/ - *.epitech.es
[2023-01-09T11:02:44.146725] https://oak.ct.letsencrypt.org/2023/ - mail.test-epitech.fr
[2023-01-09T11:03:42.091174] https://ct.googleapis.com/logs/argon2023/ - mail.test-epitech.fr
[2023-01-09T11:03:42.370193] https://ct.googleapis.com/logs/xenon2023/ - mail.test-epitech.fr
[2023-01-09T11:09:41.077546] https://oak.ct.letsencrypt.org/2023/ - epitech-listenbourg.eu
[2023-01-09T11:09:53.939987] https://oak.ct.letsencrypt.org/2023/ - back.epitech-listenbourg.eu
[2023-01-09T11:10:43.348418] https://ct.googleapis.com/logs/xenon2023/ - epitech-listenbourg.eu
[2023-01-09T11:10:45.104985] https://ct.googleapis.com/logs/xenon2023/ - back.epitech-listenbourg.eu
[2023-01-09T11:10:56.841328] https://ct.googleapis.com/logs/argon2023/ - back.epitech-listenbourg.eu
[2023-01-09T11:30:53.993648] https://ct.cloudflare.com/logs/nimbus2023/ - mail.test-epitech.fr
[2023-01-09T14:07:00.740482] https://oak.ct.letsencrypt.org/2023/ - epitech.co.uk
[2023-01-10T09:35:31.263464] https://ct.googleapis.com/logs/argon2023/ - *.epitech.in
[2023-01-11T00:35:00.162896] https://oak.ct.letsencrypt.org/2023/ - www.epitech.se
[2023-01-11T00:36:04.184545] https://ct.googleapis.com/logs/argon2023/ - www.epitech.se
[2023-01-11T00:59:12.763954] https://ct.googleapis.com/logs/xenon2023/ - epitechdszc.hu
[2023-01-11T00:59:25.319107] https://ct.googleapis.com/logs/xenon2023/ - epitechdszc.hu
[2023-01-11T03:36:38.320796] https://ct.googleapis.com/logs/xenon2023/ - phpmyadmin.epitech.se
[2023-01-11T03:36:52.618604] https://ct.googleapis.com/logs/argon2023/ - phpmyadmin.epitech.se
[2023-01-11T16:20:37.591596] https://oak.ct.letsencrypt.org/2023/ - hepitechno.repl.co
[2023-01-11T16:21:28.908667] https://ct.googleapis.com/logs/xenon2023/ - hepitechno.repl.co
[2023-01-11T16:26:22.671338] https://ct.googleapis.com/logs/xenon2023/ - *.polstimomsepitech.ga
[2023-01-11T16:26:32.463535] https://ct.googleapis.com/logs/argon2023/ - *.polstimomsepitech.ga
[2023-01-12T05:11:32.020822] https://oak.ct.letsencrypt.org/2023/ - codingclub.epitech.eu
[2023-01-12T05:12:25.158628] https://ct.googleapis.com/logs/xenon2023/ - codingclub.epitech.eu
```



AlienVault OTX API Key.  
BinaryEdge.io API Key.  
CertSpotter API key.  
FullHunt API key.  
Grayhat Warfare API key.  
Host.io API Key.  
Hunter.io API key.  
IntelligenceX API key.  
NetworksDB API key.  
Onyphe access token.  
Pulsedive API Key.  
SecurityTrails API key.  
SHODAN API Key.  
ViewDNS.info API key.  
VirusTotal API Key.  
Whoxy.com API key.



AbuseIPDB : [abuseipdb.com](https://abuseipdb.com)  
 AlienVault : [otx.alienvault.com](https://otx.alienvault.com)  
 GreyNoise : [viz.greynoise.io](https://viz.greynoise.io)  
 Host.io : [host.io](https://host.io)  
 Hybrid Analysis : [hybrid-analysis.com](https://hybrid-analysis.com)  
 Shodan : [shodan.io](https://shodan.io)  
 VirusTotal : [virustotal.com](https://virustotal.com)



GET [VirusTotal]: https://www.virustotal.com/api/v3/urls/ Response Send

200 OK 1.85 s 355.3 KB 3 Months Ago

Body Auth Query Headers Docs

URL PREVIEW  
https://www.virustotal.com/api/v3/urls/29e714ff62dee932d137dcd33e2f51789d4483f3323c89913e9036ae72abd97f/:relationship?relationship=communicating\_files  
Add Delete All Toggle Description

relationship communicating\_files  
Import from URL Bulk Edit

Preview Headers Cookies Timeline

1 [ 2 "068558435b54a67b1649601b2dbf8022850915824fc99579be3c009ebacabf4c", 3 "1159a258561cc392bb27d4c545c907f621f56b0dda6ca6c4966e638edf5156a6", 4 "126e053a148e8da83c41bb1139c9ed8fbf3dd4709601b74bb90ab261099f644", 5 "1294b908eda7cd76ad40988b943170f501f0184b503214feb1602768f8081874", 6 "1641a9b965cb58738f6dc8dba6c05645364968c498834d0e674fad8d9ce75a9", 7 "1b3c98b22e1fbae8f14caae6edf23f0e41f472dd205f595554a12abea63118e8", 8 "1bb4a3a0088cd2dca84edd32fbeb2e1e25d26ac7d79eba6167539f7dd91ddaf4", 9 "2c6bcb176e97c949080a38f5710d2b656648673dabfed14a8b9a4a77a91ffde", 10 "300cce88f0277d77ee8b97e2d5cc0060b2a9a202c491283e5f508027409ca025", 11 "35675af8739658be7c59eeb4c9484718cd9e05628491cd54355121219a0a30d26" 12 ]

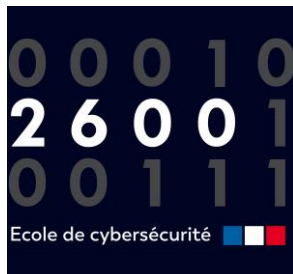
\$.data["\*"].attributes.sha256

# DEFI 4

(OSINT ON)

# Document

## Matériel :



## Règles :

- Enumération nom de domaine
- Enumération sous-domaine
- Enumération CNAME (Canonical Name)
- Enumération NS (Name Server)
- Enumération MX (Mail Exchanger)
- Enumération Registrar et Registrant
- Enumération pDNS

## Durée :

20 min

MERCI POUR VOTRE ATTENTION