

COURS OSINT

25.01.2023



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
SEC-OSI_2_01	Employer des opérateurs de recherche avancés	 RNCP_CO13	 RNCP_AC04	 RNCP_BLK03	2	 OSINT
SEC-OSI_2_02	Concevoir une investigation numérique à base de source ouverte ciblant un acteur ou une organisation.	 RNCP_CO04	 RNCP_AC02	 RNCP_BLK01	2	 OSINT
SEC-OSI_2_03	Évaluer les différents outils en source ouverte à des fins d'investigations numériques.	 RNCP_CO07	 RNCP_AC03	 RNCP_BLK02	2	 OSINT
SEC-OSI_2_04	Formaliser les résultats d'une investigation	 RNCP_CO03	 RNCP_AC01	 RNCP_BLK01	2	 OSINT
SEC-OSI_2_05	Restituer oralement les résultats d'une investigation	 RNCP_CO03	 RNCP_AC01	 RNCP_BLK01	2	 OSINT

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 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.

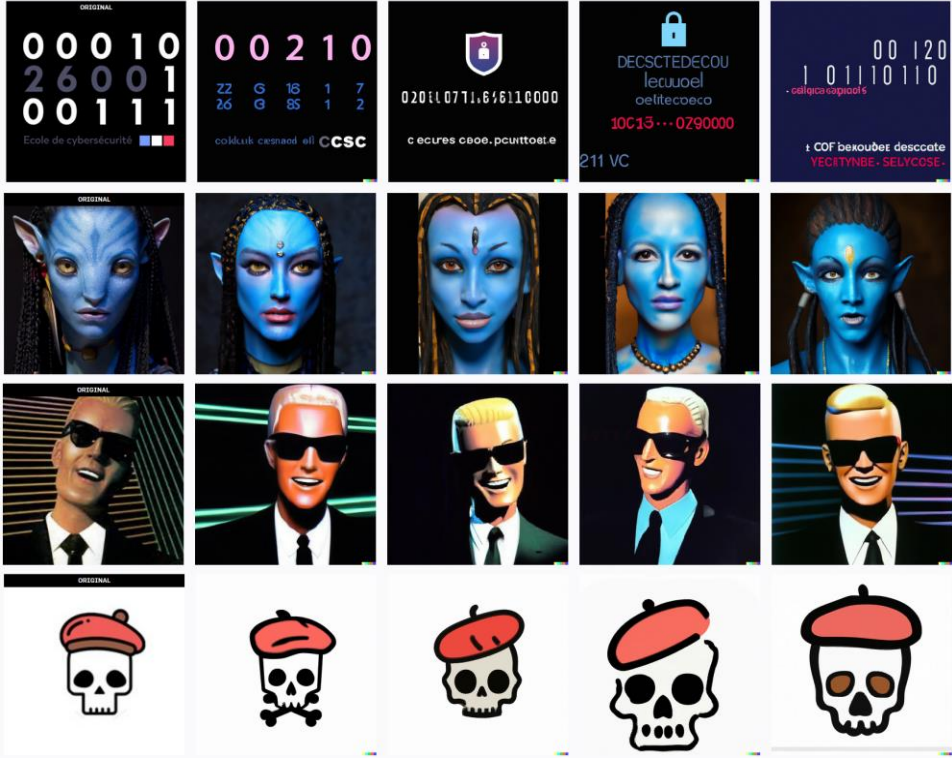
Devoirs non rendus ou rendus en retard

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

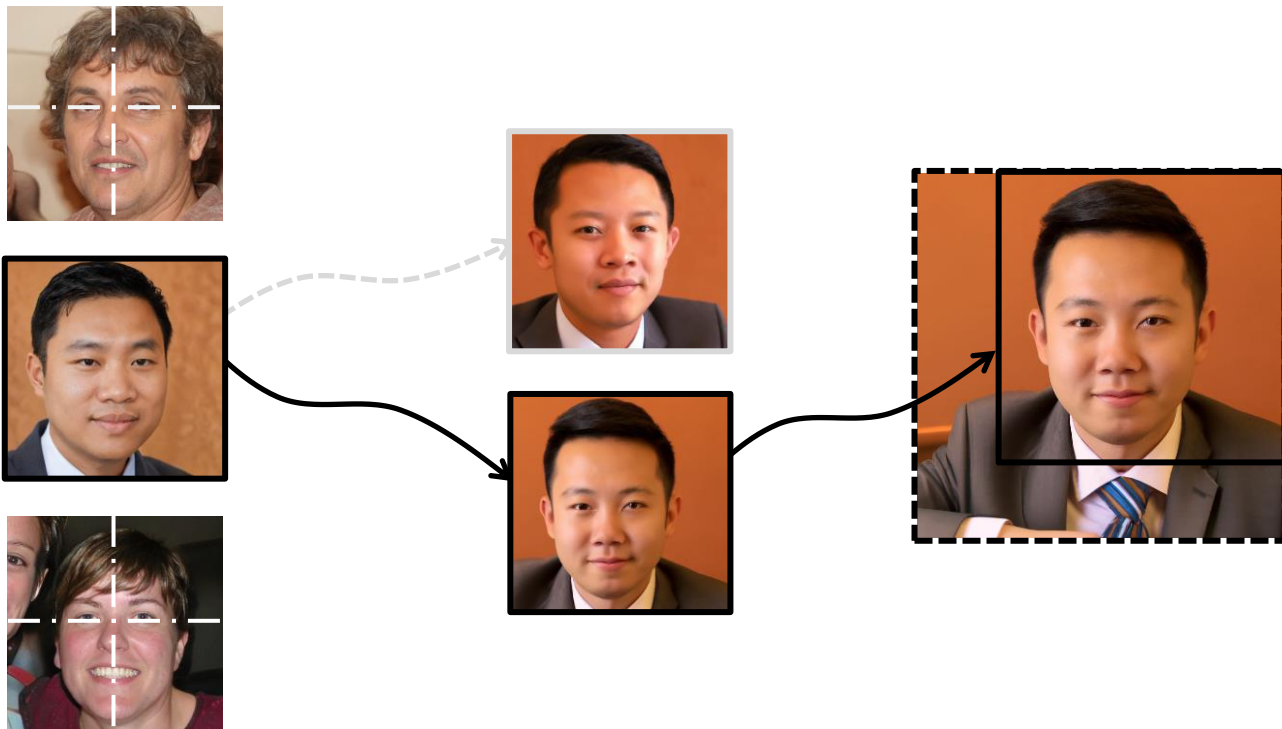
Tout devoir rendu au-delà des délais impartis se verra sanctionné par une pénalité d'1 niveau dans l'échelle de notation avec pour minimal le niveau 1.

SOCKPUPPET

AVATAR



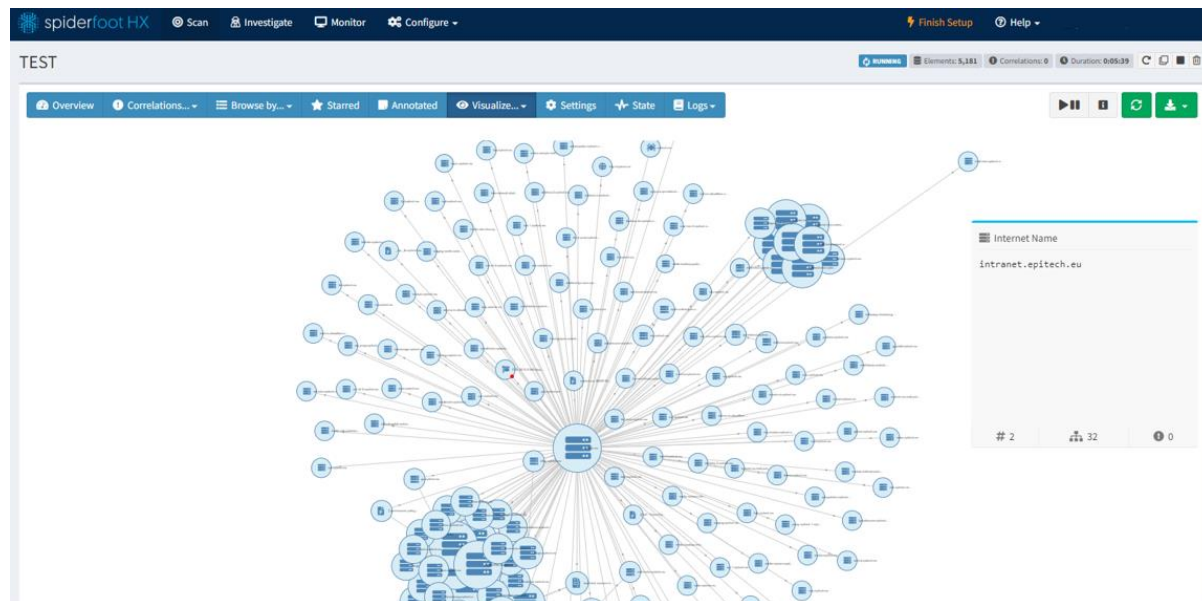
AVATAR



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/ - hepитеchno.repl.co
[2023-01-11T16:21:28.908667] https://ct.googleapis.com/logs/xenon2023/ - hepитеchno.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
```



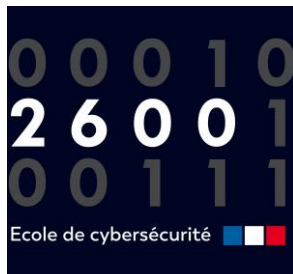
AlienVault OTX API Key.
BinaryEdge.io API Key.
CertSpotter API key.
FullHunt API key.
Grayhat Warfare API key.
Host.io API Key.
Hunter.io API key.
IntelligenceX API key.
NetworksDB API key.
Onyphe access token.
Pulsedive API Key.
SecurityTrails API key.
SHODAN API Key.
ViewDNS.info API key.
VirusTotal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

DEFI 4

(OSINT ON)

Document

Matériel :



Règles :

- Enumération nom de domaine
- Enumération sous-domaine
- Enumération NS (Name Server)
- Enumération MX (Mail Exchanger)
- Enumération Registrar et Registrant
- Enumération pDNS
- Interpréter deux valeurs issu du scan Spiderfoot et les lister dans le Google Form

Durée :

20 min



- AbuseIPDB : abuseipdb.com
- AlienVault : otx.alienvault.com
- GreyNoise : viz.greynoise.io
- Host.io : host.io
- Hybrid Analysis : hybrid-analysis.com
- Shodan : shodan.io
- VirusTotal : 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 "126e053a148e8da83c41bbc1139c9ed8fbf3dd4709601b74bb90ab261099f644", 5 "1294b908eda7cd76ad40988b943170f501f0184b503214feb1602768f8081874", 6 "1641a9b965cb58738f6dc8dba6c05645364968c498834d0e674fad8d9ce75a9", 7 "1b3c98b22e1fbae8f14caae6edf23f0e41f472dd205f595554a12abea63118e8", 8 "1bb4a3a0088cd2dca84edd32fbeb2e1e25d26ac7d79eba6167539f7dd91ddaf4", 9 "2c6bcbcb176e97c949080a38f5710d2b056648673dabfed14a8b9a4a77a91ffde", 10 "300cce88f0277d77ee8b97e2d5cc0060b2a9a202c491283e5f508027409ca025", 11 "35675af8739658be7c59eeb4c9484718cd9e05628491cd54355121219a0a30d26" 12]

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

RAPPORT



Type de rapport	
Source	CERT-OWN
Date de création	09/12/2022
Date de mise à jour	n/a
Reference	

TIP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TIP, AMBER+STRACK restricts sharing to the organization only. Sources may use TIP, AMBER when information requires support to be effectively valued upon, yet cannot risk its privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TIP, AMBER.

PAP: AMBER. Recipients may use PAP, AMBER information for conducting follow checks, like using services provided by third parties (e.g. VirusTotal), or set up a monitoring homepage.

TIP-AMBER

PAP-AMBER

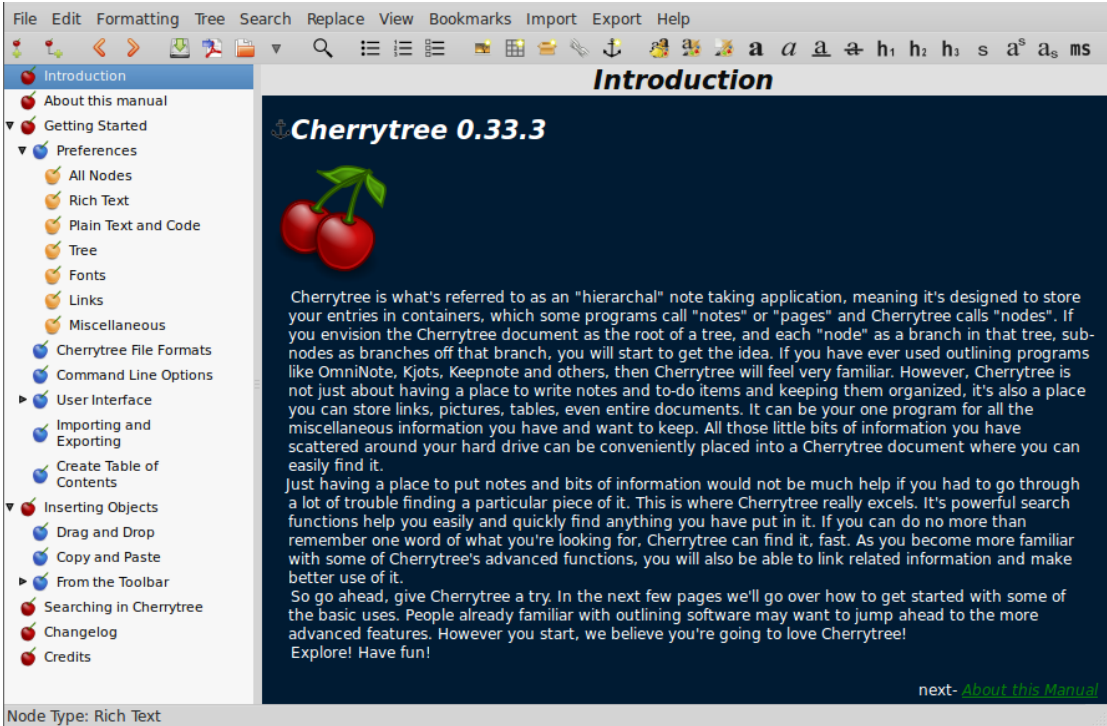


- **Texte enrichi** (couleur de premier plan, couleur d'arrière-plan, gras, italique, souligné, barré, petit, h1, h2, h3, indice, exposant, espace fixe)
- **Coloration syntaxique** prenant en charge plusieurs langages de programmation
- **Gestion des images** : insertion dans le texte, édition (redimensionnement/rotation), enregistrement en fichier png
- **Gestion des fichiers embarqués** : insertion dans le texte, sauvegarde sur disque
- Gestion des listes multi-niveaux (à puces, numérotées, à faire et basculer entre elles, multilignes avec SHIFT+ENTER)
- **Gestion simple des tableaux** (cellules avec texte brut), couper/copier/coller une ligne, importer/exporter en tant que fichier csv
- **Gestion des hyperliens** associés à du texte et des images (liens vers des pages web)
- **Vérification orthographique** (avec pygtkspellcheck et pyenchant)
- **Imprimer et enregistrer** en fichier pdf / un nœud / des sous-nœuds / l'ensemble de l'arbre
- **Export en html** d'une sélection / nœud / sous-nœuds / toute l'arborescence
- **Export en texte brut** d'une sélection / nœud / sous-nœuds / toute l'arborescence
- **Génération de data structure** pour un nœud / sous-nœuds / l'arbre entier, basé sur h1, h2 et h3
- **Protection par mot de passe** via 7-zip

github.com/giuspen/cherrytree

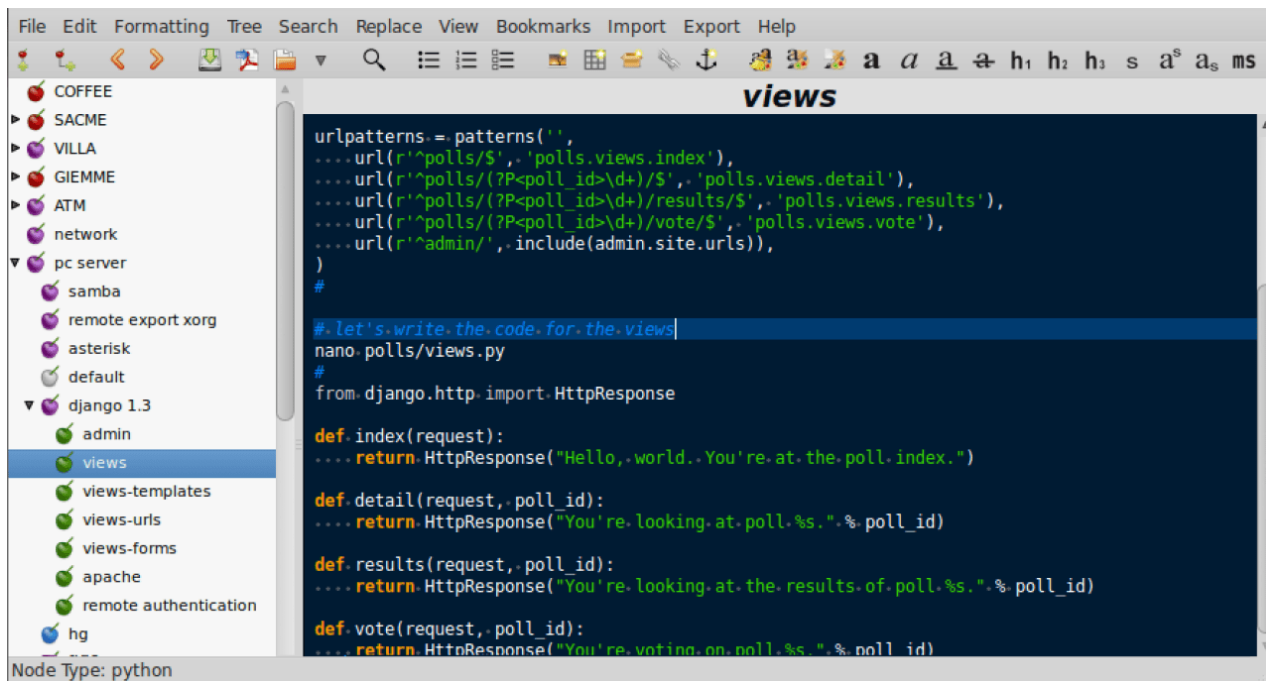


CherryTree





CherryTree





Hunchly 2.3.1

Unassigned

Search

?

⚙️

Case

To Do

Export

Unassigned

Created
April 14, 2022
11:02 AM

Active Case

Pages viewed
0

Searches
0

Captioned images
0

Selector matches
0

Notes taken
0

Selectors 0

Tags 0

+ Add

+ Bulk add

Export matches

Selector

Count

History 0

Notes 0

Images 0

Attachments 0

Searches 0

Data 0

☐ Showing 0 of 0 total pages

Sort by Newest

★

Search titles and URLs

Source : hunch.ly



Hunchly 2.3.1

Created
April 14, 2022
12:03 PM

Active Case

17

2

Captioned images

0

Selector matches

14

Notes taken

0

Tag

Tagged Pages

Social Media

1

Imagery of Weapons

0

History 17

Notes 0

Images 0

Attachments 0

Searches 2

Data 80

☐ Showing 17 of 17 total pages

Sort by Newest



Search titles and URLs



Justin Seitz (@jms_dot_py) / Twitter

https://twitter.com/jms_dot_py?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

April 14, 2022 12:25 PM

Justin Seitz, jms_dot_py

Social Media



justin seitz - Google Search

https://www.google.com/search?q=justin+seitz&source=hp&ei=zFdYYr2BLeGu0PEpm8Oy0Ac&fifsig=AHkkrS4AAAAAYIhI3EoSj0lpzQtP_oU61YEnlrkGKypH&ved=0ahUKEwi9I9...

www.hunch.ly



- Editeur de texte en Markdown.
- Application de base de connaissances
- Stocker vos propres fichiers sur votre ordinateur.
- Le cerveau humain n'est pas linéaire
- Toutes les informations sont stockées dans un répertoire au format Markdown
- disponible MacOS, Windows, Linux mais aussi pour les smartphones via l'App Store (IOS) ou le Play Store (Android)



Source : obsidian.md



td-architecture - Obsidian v0.12.12

Graph view

td-architecture

- Architecture
- Capability-Groups
- Cloud-Management
- FAQ
- Icons
- Models
 - Archi User Guide
- Architecture-Models
- Obsidian-Settings
- OS-Values
- Partners
- Patterns
- Principles-Policies-and-Standards
- References
- Scripts
- Systems-and-Services
- Technology
- Templates
- Architecture
- Capability-Groups
- Cloud-Management
- FAQ
- Hello-World

Architecture-Models

Archi

The Open Group Modeling tool used to create Models in Architecture is called Archi and is available to download from the OS App Portal which is [here](https://osappportal.esd/items/Details?PackageId=2258)(<https://osappportal.esd/items/Details?PackageId=2258>).

****Please Note:**** _You will need to connect to the VPN to gain access to the OS App Portal_

coArchi Plug in

Installation of the coArchi Plug in ****is required**** to allow Archi access to Git compatible change control, ie the T&D Repository where our models are stored, allowing for multi-user collaboration on these models.

Aug 2021 < TODAY >

MON	TUE	WED	THU	FRI	SAT	SUN
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

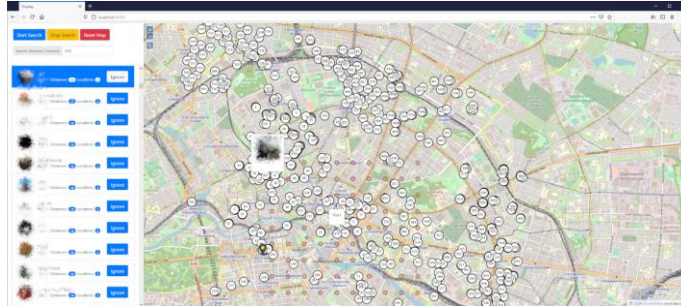
Type to start search...

1 backlink 480 words 3638 characters

SOCMINT



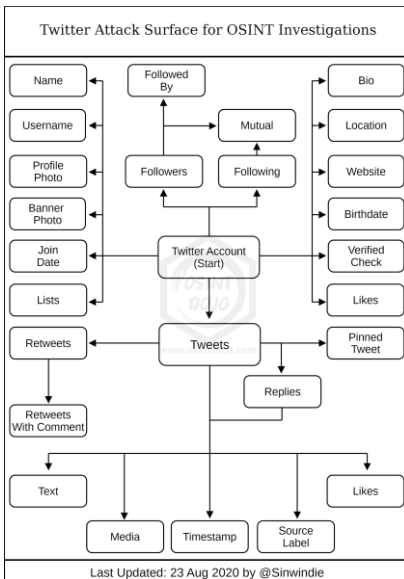
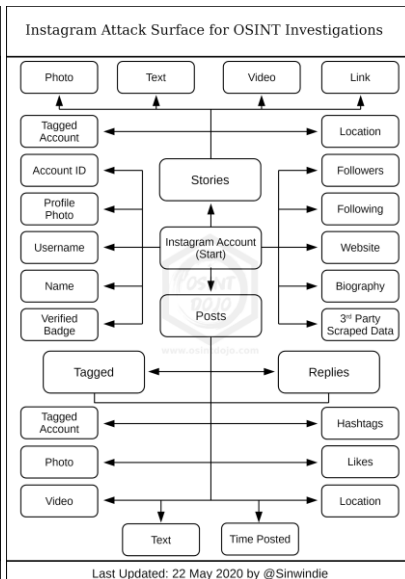
- github.com/jordanwildon/Telepathy : enquêter sur les chats Telegram
- github.com/pigpagnet/save-telegram-chat-history : Enregistrer l'historique des conversations
- github.com/odysseusmax/tg-index : Indexez un ou plusieurs canaux/chats
- github.com/TGViewer/TGViewer.github.io : Partagez votre publication sur Internet
- github.com/Forichok/TelegramOnlineSpy : alerte si l'un des utilisateurs de la liste a changé son statut en ligne
- github.com/paulpierre/informer : se faire passer pour plusieurs utilisateurs (base de données MySQL)
- github.com/pielco11/telescan : utilisateurs dans des groupes par identifiant, nom ou numéro de téléphone
- github.com/jkctech/Telegram-Trilateration : résultats de 500 m, 1 km, 2 km
- github.com/Alb-310/Geogramint : utilisateurs et groupes à proximité
- github.com/tejado/telegram-nearby-map : utilisateurs de Telegram qui ont activé la fonctionnalité à proximité.
- ...

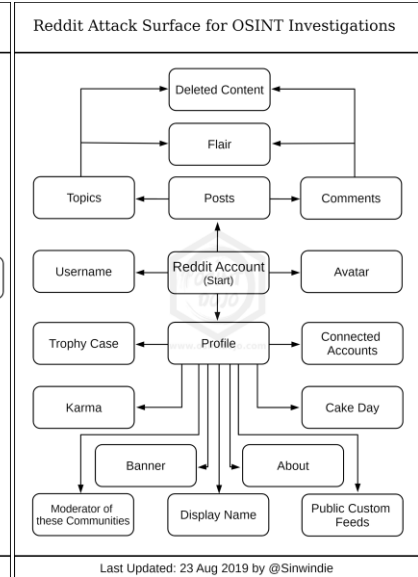
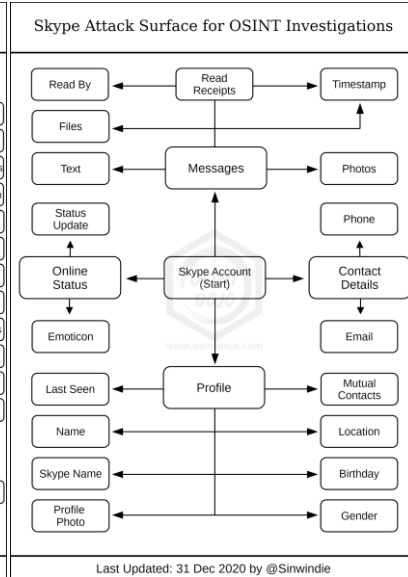
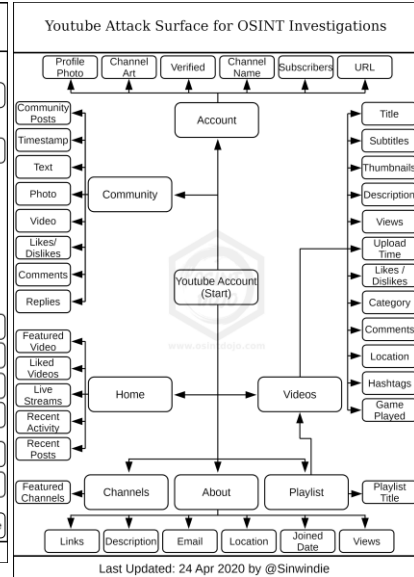
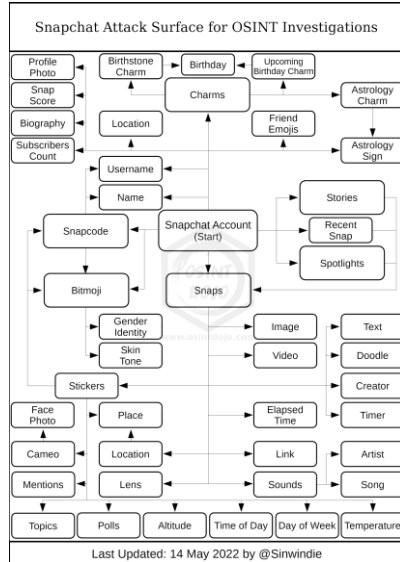


t.me/username -site:telegram.org

t.me/s/username

t.me/joinchat/<hash> -site:telegram.org





OUTILS



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





- github.com/kpcyrd/sn0int : **sn0int.com**
 - github.com/soxoj/maigret : vérification des comptes sur un grand nombre de sites
 - github.com/sherlock-project/sherlock : vérification des comptes sur un grand nombre de sites
 - github.com/twintproject/twint : Twitter scraping
 - github.com/mxrch/Ghunt : offensive Google framework (email, ID, fichier Drive),
 - github.com/qeeqbox/social-analyzer : profil d'une personne via 1000 sources
 - github.com/smicallef/spiderfoot : threat intelligence
 - github.com/sundowndev/phoneinfoga : framework pour numéro de telephone
 - github.com/OWASP/Amass : Cartographie de la surface d'attaque et découverte d'actifs
 - github.com/megadose/holehe : recherche de mail sur différents sites (fonction mot de passe oublié)
-
- github.com/jivoi/awesome-osint
 - github.com/edoardottt/awesome-hacker-search-engines
 - github.com/giuliacassara/awesome-social-engineering
 - github.com/redhuntlabs/Awesome-Asset-Discovery
 - github.com/ARPSyndicate/awesome-intelligence

DEFI 5

(OSINT ON)

Document

Matériel :



Règles :

- Identifier le site internet du magazine 2600: The Hacker Quarterly
- Retrouver au moins 26 adresses mail appartenant ou ayant appartenu à 2600
- Identifier l'adresse postale en 2023 et celle de 1996
- Identifier les compte Twitter, Facebook, Youtube, Mastodon et Instagram
- Récupéré la PGP PUBLIC KEY
- Retrouver la date exacte de sortie de prison de Bernie S.

Durée :

30 min

DEFI 6

(OSINT ON)

Document

- Matériel :



Règles :

- Retrouver les BSSID 7 des SSID 3 SSID suivant ecole2600, ecole2600_guest et ecole2600_students_24, via le service en ligne <https://wigle.net>.
- Récupérer en même temps, les longitudes et latitudes associées à chaque BSSID.

Durée :

20 min

MERCI POUR VOTRE ATTENTION