Avant propos :

Ce cours s'adresse à des autodidactes qui souhaitent se former à l'OSINT en partant des bases, pour progresser pas à pas jusqu'à une maîtrise suffisante leur permettant de décrocher un premier poste d'analyste OSINT junior.

Je pars donc du principe que si tu lis ces lignes, c'est que tu es un débutant complet.
En ce sens, permets-moi de te prévenir d'avance : beaucoup de termes et de notions te sembleront obscurs au premier abord, et c'est normal.

Même si ces cours ont pour objectif de structurer un apprentissage souvent chaotique lorsqu'on débute seul, ils s'inscrivent pleinement dans l'esprit et la philosophie autodidacte. Cela signifie que je t'invite à chercher par toi-même à comprendre et à assimiler chaque nouveau concept, outil ou idée dont tu ignores encore le sens. Tu les découvriras au fil de ta lecture.

Tu peux, pour cela, t'entraîner à l'OSINT en effectuant tes propres recherches sur le web, ou même demander à l'une des nombreuses IA gratuites disponibles de t'expliquer ce qui t'échappe.
Personnellement, lorsque je tombe sur un concept que je ne comprends pas, je cherche à le relier à d'autres que je maîtrise déjà, puis je crée une fiche de révision selon un format que tu trouveras dans la section *"Outils"* de ma page GitHub.

Si tu n'es pas moteur dans ton apprentissage, alors ce cours ne te servira à rien.
Mais si tu prends le temps d'être curieux, d'expérimenter et de comprendre plutôt que de réciter, alors je te promets que ces cours te guideront pas à pas jusqu'à un niveau professionnel.

Remerciements:

Il y a certaines personnes qui jouent le rôle de boussole dans nos vies.
La mienne, dans mon apprentissage de l'OSINT, s'appelle Adrien Rouillon, alias *Anadema*. C'est un professionnel de la cybersécurité qui m'a tendu la main, m'a transmis beaucoup de savoir, et m'a aidé à garder le cap lorsque la tempête se déchaînait sur mon chemin autodidacte.

Je tiens donc à le remercier chaleureusement pour avoir contribué à donner vie à Jäger. Anadema a pris le temps de créer des ressources précieuses pour les personnes désirant se former à l'OSINT. Je t'invite vivement à les consulter en parallèle de mes cours, à l'adresse suivante : https://github.com/Anadema/

Amicalement,
Jäger

djagerosint@proton.me

Chapitre 1 : Qu’est-ce qu’Internet ?

(Phase 1 – Module 1 – Partie 1 : Anatomie d’Internet)

1. Introduction : L’illusion du nuage

Quand on parle d’Internet, beaucoup imaginent un “nuage” flottant dans l’air, un espace invisible où vivent les sites web, les vidéos et les messages.
Mais Internet n’a rien d’un nuage : c’est un monstre physique, un réseau de réseaux, une machine mondiale faite de câbles, de serveurs, de routeurs et d’échanges électriques.

Tout ce que tu fais en ligne (envoyer un message, publier une photo, faire une recherche) transite dans un monde matériel.
Et un analyste OSINT, lui, apprend à lire les traces laissées dans cette matière.

2. Internet, c’est quoi exactement ?

Internet = inter-network → un réseau de réseaux.

Imagine une gigantesque ville mondiale :

- Les routes : ce sont les câbles, fibres, antennes et routeurs qui relient tout.
- Les maisons : ce sont les ordinateurs, serveurs, smartphones, objets connectés.
- Les adresses : ce sont les adresses IP qui permettent de localiser chaque maison.
- Les panneaux de signalisation : ce sont les DNS, qui traduisent les noms en adresses.
- Et les véhicules qui circulent : ce sont les paquets de données, les petits bouts de ton message découpés et envoyés à destination.

Quand tu navigues sur un site, ton ordinateur n’invoque pas de magie :
il emprunte un itinéraire à travers cette ville numérique pour aller chercher l’information.

3. L’infrastructure physique : le squelette d’Internet

Tout commence par le matériel :

- Les câbles sous-marins : des milliers de kilomètres reliant les continents (ils transportent plus de 95 % du trafic mondial).
- Les routeurs et les data centers : les “carrefours” où les données changent de direction.
- Les FAI (fournisseurs d’accès Internet) : les portes d’entrée qui te connectent à la ville mondiale.

Rien n’est vraiment “virtuel” : chaque clic traverse des bâtiments, des machines, des continents.

Quand tu regardes un site américain depuis la France, ta requête voyage littéralement sous l'océan avant de revenir.

4. Internet, c'est aussi des règles : les protocoles

Pour que tout ce monde hétérogène fonctionne ensemble, il faut des règles communes, appelées protocoles.
C'est comme une langue universelle que toutes les machines comprennent.

Quelques exemples :

- **IP** (Internet Protocol) → indique l'adresse de chaque machine.
- **TCP** (Transmission Control Protocol) → découpe et réassemble les messages.
- **HTTP / HTTPS** → gère la communication entre ton navigateur et un site web.
- **SMTP** → pour les emails.
- **DNS** → pour traduire les noms en adresses.

Sans ces règles, Internet serait une foule d'ordinateurs qui ne se comprennent pas.

5. Internet n'est pas le Web

Le Web n'est qu'un quartier d'Internet.

Internet, c'est la ville entière ;
le Web, c'est juste un ensemble de rues dédiées aux pages web.
D'autres "quartiers" existent : les emails, le FTP, la messagerie instantanée, les bases de données, etc.

Tu peux donc être "sur Internet" sans être "sur le Web".
C'est important pour l'OSINT : toutes les données exploitables ne viennent pas du Web.
Les leaks, les registres, les métadonnées, les fichiers ouverts — tout ça vit *hors du Web visible.*

6. Internet vu par un analyste OSINT

Pour un analyste, Internet est une cartographie vivante de relations :

- Chaque site, chaque serveur, chaque adresse IP raconte une histoire.
- Derrière chaque domaine, il y a un propriétaire, un hébergeur, un fournisseur, un emplacement physique.
- Derrière chaque connexion, une suite de protocoles laisse des empreintes techniques (IP, DNS, headers, certificats…).

L'enquêteur OSINT n'invente rien : il observe, relie, et interprète les traces laissées par ce réseau mondial.

7. Résumé : “Explique Internet à un enfant”

“Internet, c’est comme un réseau de routes reliant tous les ordinateurs du monde.
Ton ordinateur envoie des petits colis appelés paquets.
Ces paquets voyagent de routeur en routeur jusqu’à trouver la maison du destinataire.
Chaque maison a une adresse unique, qu’on appelle IP.
Et pour éviter de retenir ces chiffres, on a inventé des noms, que le DNS traduit pour nous.
Voilà : Internet, c’est le facteur du monde moderne.”

8. Mini-exercice : dessine Internet

But : visualiser sa structure physique et logique.

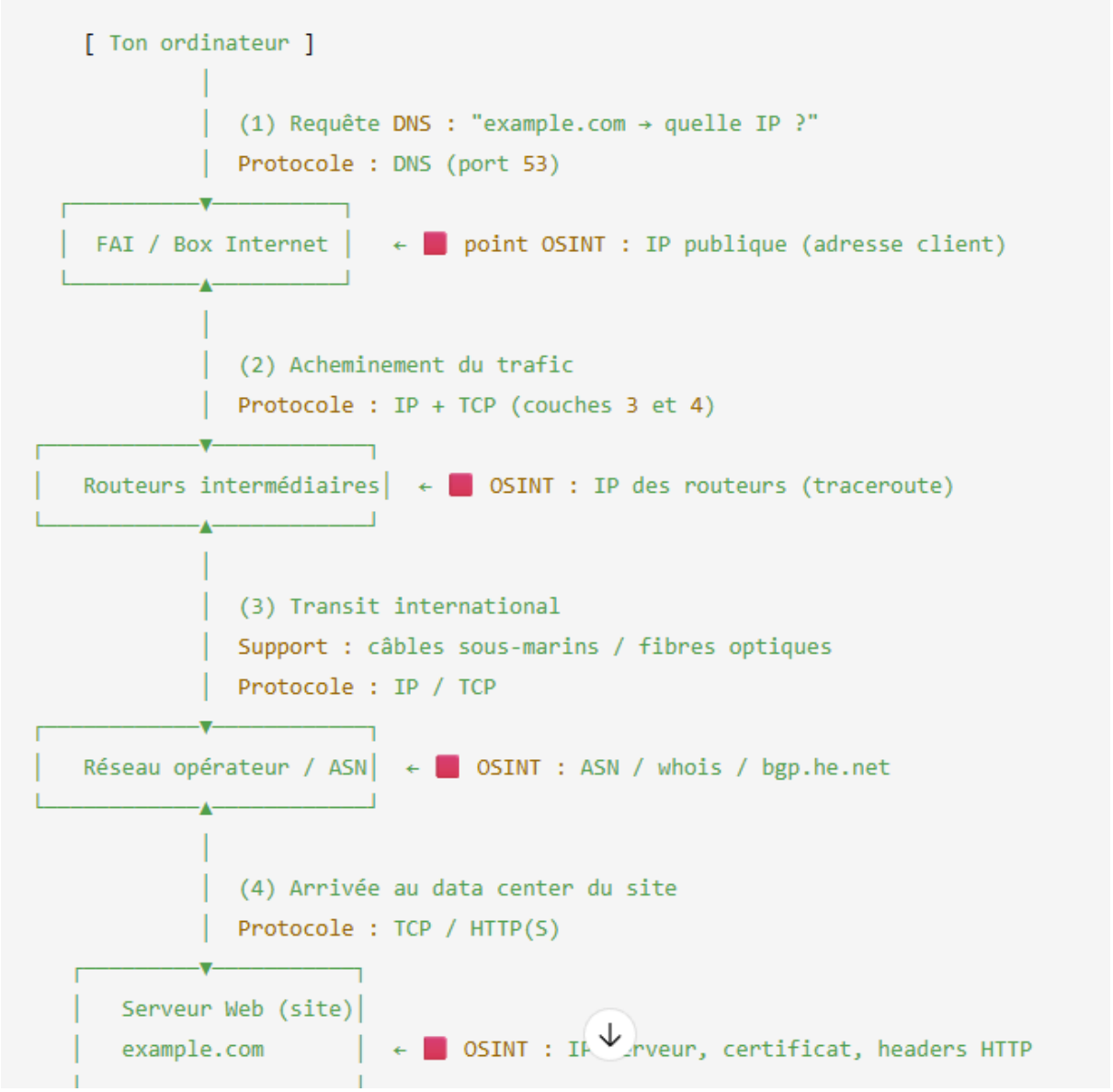
Consignes :

1. Dessine ton ordinateur à gauche, et un serveur de site web à droite.
2. Relie-les par des flèches représentant :
    - ton fournisseur d’accès (FAI),
    - les routeurs intermédiaires,
    - les câbles sous-marins,
    - le data center du site.
3. Sur chaque flèche, note le type de protocole (DNS, IP, TCP, HTTP).
4. Entoure en rouge les points où un analyste OSINT pourrait observer des informations.

Tu viens de **cartographier Internet** à l’échelle d’une requête.

La correction est sur la page suivante du cours !

Corrections :



🧾 9. Ce qu'il faut retenir

Notion	Résumé
Internet	Un réseau mondial reliant des millions de réseaux entre eux.
Web	Une partie d'Internet (pages, navigateurs, HTTP/HTTPS).
IP	L'adresse numérique d'une machine.
DNS	L'annuaire qui relie les noms aux adresses.
OSINT	L'art d'exploiter les traces laissées sur ce réseau.

10. À ce stade, tu dois savoir :

- Expliquer simplement ce qu'est Internet.
- Faire la différence entre "Internet" et "Web".
- Visualiser le réseau comme un monde physique (machines, câbles, adresses).
- Comprendre que l'OSINT consiste à exploiter ces traces visibles.
-

Chapitre 2 : Différence entre Internet, le Web et l'OSINT

(Phase 1 – Module 1 – Partie 1 : Anatomie d'Internet)

1. Pourquoi cette distinction est cruciale

Beaucoup utilisent les mots *Internet* et *Web* comme des synonymes.
C'est une erreur classique, et elle empêche de comprendre où se cachent réellement les données exploitables en OSINT.

L'Internet, c'est le tout.
Le Web, c'est une partie.
Et l'OSINT, c'est une méthode pour explorer intelligemment ce tout.

2. Internet : la ville entière

“Internet, c’est le monde physique et logique de toutes les communications numériques.”

Tu peux voir Internet comme une mégapole mondiale.
Elle contient :

- des routes (les câbles, fibres, routeurs) ;
- des bâtiments (serveurs, ordinateurs, objets connectés) ;
- et des règles de circulation (protocoles IP, TCP, UDP…).

Tout ce qui transmet des données, même sans passer par un navigateur web, fait partie d’Internet :

- les mails,
- les transferts de fichiers,
- les appels VoIP,
- les jeux en ligne,
- les bases de données,
- et même les caméras connectées.

Internet, c’est l’infrastructure — la toile invisible.

3. Le Web : un quartier particulier d’Internet

“Le Web, c’est la partie d’Internet à laquelle on accède avec un navigateur.”

Quand tu ouvres Firefox, Edge ou Chrome, tu utilises un protocole : HTTP ou HTTPS.
C’est ce protocole qui t’emmène sur des pages.

Le Web, c’est donc :

- des sites (pages HTML, CSS, JavaScript) ;
- des serveurs web (Apache, Nginx, IIS) ;
- des noms de domaine (`example.com`) ;
- et des liens hypertexte reliant ces pages.

C’est ce qu’on appelle parfois le “World Wide Web”, inventé par Tim Berners-Lee en 1989.

IMPORTANT = Le Web est donc une application d’Internet — pas Internet lui-même.

Sans Internet, le Web ne pourrait pas exister.
Mais sans Web, Internet continuerait très bien à vivre (grâce aux mails, FTP, messageries, etc.).

4. L’OSINT : la méthode d’enquête sur ce monde

“OSINT, c’est l’art d’exploiter les données accessibles publiquement sur Internet.”

L’OSINT ne se limite pas au Web visible.
Un bon analyste explore tous les étages accessibles légalement :

- Le Web visible (sites, réseaux sociaux, forums)
- Le Web profond (bases de données non indexées, documents, API)
- Les traces techniques (WHOIS, DNS, certificats, métadonnées, IP exposées)
- Les sources ouvertes non web : fichiers PDF publics, registres légaux, dépôts GitHub, etc.

L’OSINT ne consiste donc pas à “naviguer” sur Internet, mais à l’observer, l’analyser, le recouper.
L’Internet est ton terrain de jeu, le Web est un de ses quartiers, et toi, tu es l’enquêteur.

5. Une analogie simple : la ville, le quartier et l’enquêteur

Élément	Analogie urbaine	Description
Internet	La ville entière	Routes, bâtiments, énergie, transports : tout ce qui relie et fait circuler l’information.
Web	Un quartier	L’espace “public” des vitrines, panneaux et boutiques (les sites web).
OSINT	Le détective	Celui qui arpente la ville, observe les panneaux, interroge les registres, et relie les indices.

6. Pourquoi les débutants confondent tout

Parce que le Web est la seule partie visible du réseau pour 99 % des gens.
Quand on ouvre un navigateur, on pense être “sur Internet”.
En réalité, on n’en voit qu’une façade polie et limitée.

L’analyste OSINT, lui, apprend à regarder derrière la façade :

- qui héberge la boutique ?
- où mènent les tuyaux derrière ?
- qui est propriétaire du bâtiment ?
- quelles traces techniques révèlent son activité ?

7. Le Web visible, le Web profond, le Web obscur

Une autre confusion courante vient de ces trois termes, qu’il faut clarifier dès maintenant :

Terme	Définition claire	Exemples	OSINT possible ?
Web visible (Surface Web)	Indexé par Google, accessible publiquement	Wikipédia, médias, sites d’entreprises	✅ Oui, c’est la base
Web profond (Deep Web)	Accessible mais non indexé (bases, intranets, API, documents non référencés)	Google Drive privé, archives, forums non publics	⚠️ Oui, sous conditions légales
Web obscur (Dark Web)	Nécessite un logiciel spécifique (Tor, I2P)	Marchés noirs, forums cachés	⚠️ Oui, mais très encadré et risqué

IMPORTANT : Le Web visible ne représente que **4 à 5 %** du contenu total d’Internet.
Tout le reste dort sous la surface.

8. Internet & Web : comment les OSINT Tools s'y situent

Si tu débutes, il est normal que tu ne comprennes pas entièrement le tableau qui va suivre.
Mais je te le présente maintenant afin de te lancer un petit défi : fais l'effort de le lire avec tes connaissances actuelles, puis reviens dessus lorsque tu auras fini d'apprendre le cours.
Tu pourras alors apprécier ta progression, et je suis prêt à parier que tu penseras :
« La vache, en fait c'était super simple à comprendre ! »
"

Outil	Cible principale	Couches réseau concernées
Google Dorks	Web visible & partiellement profond	Application (HTTP/HTTPS)
Maltego	Web + DNS + IP + serveurs	Application → réseau
Shodan	Internet (machines, serveurs, ports ouverts)	Couches 3–4 (TCP/IP)
Spiderfoot	Internet complet (collecte multi-source)	Toutes couches
ExifTool	Fichiers issus du Web ou hors-ligne	Application
WHOIS / DNS tools	Internet brut (infrastructure)	Couches 1–3

Un bon analyste ne reste pas enfermé dans le Web.
Il descend dans les couches inférieures du réseau pour comprendre d'où viennent les données et comment elles circulent.

9. Résumé :

"Internet, c'est l'ensemble des routes du monde numérique.
Le Web, c'est un quartier bien éclairé où tout le monde se promène.
Et l'OSINT, c'est l'enquêteur qui observe aussi les ruelles, les parkings et les registres pour comprendre ce qui se passe derrière les façades."

10. Mini-exercice : “Classifie le monde numérique”

But : apprendre à situer chaque ressource.

Consigne : Classe les exemples suivants selon qu’ils relèvent d’Internet, du Web ou des deux :

1. Un email Gmail
2. Une vidéo YouTube
3. Un résultat DNS
4. Un serveur exposé sur Shodan
5. Une page Wikipedia
6. Un document PDF trouvé sur un FTP public
7. Une conversation sur Telegram

La correction est sur la prochaine page du cours !

✅ Correction attendue :

Exemple	Internet uniquement	Web uniquement	Les deux
Un email Gmail			✅ (parce que même si les mails transitent par internet, tu les envoient probablement à partir du site HTTPS de ta boite mail.)
Une vidéo YouTube		✅ (HTTP/HTTPS)	
Un résultat DNS	✅ (DNS, port 53)		
Un serveur exposé sur Shodan	✅ (machine accessible sur Internet)		
Une page Wikipedia		✅ (HTTP/HTTPS)	
Un document PDF trouvé sur un FTP public			✅ si ce même fichier est aussi servi via HTTP (beaucoup de sites le font)
Une conversation sur Telegram			✅ si tu utilises web.telegram.org (mais le le service de messagerie en lui même passe par Internet)

11. Ce qu’il faut retenir

Concept	Résumé clair
Internet	L’infrastructure mondiale reliant tous les réseaux.
Web	Une application d’Internet qui affiche des pages.
OSINT	L’art d’exploiter les données accessibles sur l’ensemble d’Internet.
Surface / Deep / Dark Web	Trois niveaux d’accessibilité de l’information.
Vision OSINT	Comprendre le réseau au-delà du Web visible.

12. À ce stade, tu dois savoir :

- Expliquer la différence entre Internet, Web et OSINT.
- Classer les données selon leur type et leur niveau d’accessibilité.
- Comprendre pourquoi l’analyste OSINT doit explorer **au-delà des navigateurs**.
- Identifier à quel niveau chaque outil agit.

Chapitre 3 : L’architecture en couches : OSI & TCP/IP

(Phase 1 – Module 1 – Partie 1 : Anatomie d’Internet)

1. Pourquoi parler de “couches” ?

Imagine un restaurant :

- Le serveur prend ta commande,
- Le cuisinier prépare le plat,
- Le livreur l’apporte à ta table.

Chacun fait sa part, sans se soucier des détails du précédent.
Internet fonctionne pareil :

Chaque “couche” du réseau fait son travail et transmet le résultat à la suivante.

C’est ce qu’on appelle une architecture en couches — un système conçu pour que des milliards de machines différentes puissent parler le même langage sans se marcher dessus.

Le modèle OSI expliqué simplement

Imagine deux immeubles identiques :

- toi, à gauche, ton ordinateur (l’expéditeur),

- le serveur à droite (le destinataire).
  Entre vous, la “rue”, c’est Internet.

Quand tu envoies un message (une requête, un mail, une vidéo…), il descend les 7 étages de ton immeuble, traverse la rue, puis remonte les 7 étages de l’autre côté.

🧩 Couche 7 — Application (l'étage de la communication humaine)

Rôle :

C'est la partie que toi tu vois : ton navigateur, ton logiciel mail, ton appli.
C'est là que tu "parles" avec Internet.

Exemple :

Tu tapes `https://example.com` dans Chrome → ton navigateur crée une requête HTTP.

En OSINT :

- Les headers HTTP, les cookies, les formulaires, les API appartiennent à cette couche.
- Quand tu fais un `curl -I example.com`, tu observes directement la couche 7.

🧩 Couche 6 — Présentation (le traducteur)

Rôle :

Elle met en forme les données pour qu'elles soient comprises par les deux ordinateurs : encodage, chiffrement, compression, décompression…

Exemple :

Quand tu te connectes à un site HTTPS, c'est ici que le SSL/TLS chiffre la communication.
Quand tu ouvres une vidéo ou une image, c'est cette couche qui décode le format (JPEG, MP4, etc.).

En OSINT :

- Tu y trouves des infos dans les certificats TLS, visibles via `openssl s_client`.
- Un domaine avec un certificat SSL expiré → indice technique exploitable.

🧩 Couche 5 — Session (le chef d’orchestre)

Rôle :

Elle gère la session entre les deux machines : ouverture, maintien, fermeture de la communication.
Sans elle, chaque clic serait une nouvelle connexion.

Exemple :

Quand tu te connectes à un site, les cookies et les tokens gardent ta session ouverte sans te reconnecter à chaque page.
Quand tu fais une visio, c’est elle qui maintient la session tant que tu parles.

En OSINT :

- Observer les cookies, les tokens d’authentification ou les sessions ouvertes (dans les headers) donne des indices sur la structure et les technologies d’un site.

🧩 Couche 4 — Transport (le livreur fiable)

Rôle :

Elle découpe ton message en paquets, s’assure qu’ils arrivent dans le bon ordre, et qu’aucun ne manque.
C’est la garantie que “Bonjour” ne devienne pas “Bon…”.

Exemple :

- TCP (Transmission Control Protocol) = livraison fiable (ex : HTTP, mails).
- UDP (User Datagram Protocol) = plus rapide mais sans vérification (ex : streaming, jeux).

En OSINT :

- Les ports (80, 443, 22, 25…) sont gérés ici.
- Shodan, Nmap, etc. travaillent à cette couche pour repérer les services exposés.

🧩 Couche 3 — Réseau (le GPS)

Rôle :

Elle gère l'adressage et le routage.
C'est elle qui décide par où tes paquets doivent passer pour arriver à bon port.

Exemple :

- Le protocole IP (Internet Protocol) détermine les adresses IP source et destination.
- ICMP (utilisé par `ping`) vérifie la disponibilité d'une machine.

En OSINT :

- Tu exploites cette couche avec des outils comme `whois`, `ipinfo.io`, `traceroute`.
- Elle révèle les fournisseurs d'accès, les ASN, et les zones géographiques des machines.

🧩 Couche 2 — Liaison de données (la rue locale)

Rôle :

Elle permet la communication entre deux appareils sur le même réseau local (ta box et ton PC, ou deux routeurs).
Elle attribue des adresses physiques (MAC) aux appareils.

Exemple :

- Ethernet, Wi-Fi, PPP (connexion modem).
- C'est ici que transitent les "frames", les petits blocs envoyés sur un câble ou dans les airs.

En OSINT :

- Peu utilisée directement (sauf en enquêtes locales ou forensiques).
- Les adresses MAC ou SSID Wi-Fi peuvent être exploitées dans des contextes précis (géoloc, OSINT mobile).

🧩 Couche 1 — Physique (le plancher)

Rôle :

C’est le support matériel de tout : les câbles, les fibres, les signaux électriques ou optiques, les ondes radio.
Elle transforme les 0 et 1 en impulsions électriques.

Exemple :

Les câbles sous-marins, les fibres, les antennes 4G, le Wi-Fi, tout ce qui transporte physiquement l’information.

En OSINT :

- Elle n’est pas exploitable directement (sauf analyse d’infrastructures, data centers, câbles).

- Mais elle t’intéresse pour comprendre la dépendance géographique d’un site ou d’un pays (cartes de câbles, points d’échange, etc.).

3. Le modèle TCP/IP : la version réelle utilisée aujourd’hui

On va donc décortiquer ce modèle **TCP/IP** simplement, avec des métaphores claires et une logique qui complète ce que tu viens d’apprendre sur l’OSI.

L’idée est la suivante :

- Le modèle **OSI** (7 couches) est **pédagogique** — une carte pour comprendre.

- Le modèle **TCP/IP** (4 couches) est **pratique** — c’est celui que les ordinateurs utilisent réellement aujourd’hui.

Le modèle TCP/IP — la version “du monde réel”

Vue d’ensemble

Imagine que le modèle OSI, c’est un immeuble de 7 étages.
Le modèle TCP/IP, lui, **fusionne plusieurs étages pour simplifier la vie des ingénieurs**.
On garde seulement **4 grands niveaux fonctionnels** :

[Application]

[Transport]

[Internet]

[Accès réseau]

Chaque niveau correspond à **une mission précise** dans le voyage d’une donnée.
Voyons-les un par un 👇

🧩 Couche 4 : Application

(Correspond aux couches 5 à 7 du modèle OSI)

Rôle :

C'est la partie la plus haute : celle qui interagit directement avec l'utilisateur ou avec un logiciel.
Elle regroupe tout ce qui concerne les protocoles applicatifs : HTTP, HTTPS, FTP, DNS, SMTP, etc.

Image simple :

Tu écris une lettre ou tu remplis un formulaire → c'est ici.
Cette couche gère le contenu et le langage de la communication.

Exemple concret :

- Quand tu tapes une URL, ton navigateur envoie une requête HTTP/HTTPS.
- Quand tu ouvres Gmail, tu utilises SMTP/IMAP.
- Quand tu fais une recherche de domaine, ton PC parle à un serveur DNS.

En OSINT :

C'est la couche la plus "riche" en informations humaines :

- Headers HTTP (serveur, cookies, redirections).
- Contenu des pages web (source HTML).
- Certificats TLS (HTTPS).
- API ouvertes, ports applicatifs.

Exemples d'outils : `curl`, `Wappalyzer`, `BuiltWith`, `ExifTool`, `SpiderFoot`.

🧩 Couche 3 : Transport

(Correspond à la couche 4 de l'OSI)

Rôle :

C'est le chef de la logistique.
Elle s'occupe de découper, envoyer et réassembler les messages (paquets).
Elle gère aussi la fiabilité des transmissions.

Image simple :

Tu veux envoyer une grande lettre, mais elle ne rentre pas dans une seule enveloppe → tu la coupes en morceaux numérotés, tu les envoies, et le destinataire les recolle dans le bon ordre.

Protocoles clés :

- TCP (Transmission Control Protocol) : fiable, vérifie que tout est bien reçu (utile pour le Web).
- UDP (User Datagram Protocol) : plus rapide, mais sans vérification (utile pour les vidéos, jeux, DNS).

En OSINT :

- L'analyse de ports (ex : 80 = HTTP, 443 = HTTPS, 22 = SSH, 25 = SMTP) repose sur cette couche.
- C'est ici que Shodan et Nmap travaillent : ils voient quels services répondent et sur quels ports.

Exemples d'outils : Shodan, Nmap, Netcat.

🧩 Couche 2 : Internet

(Correspond à la couche 3 du modèle OSI)

Rôle :

C’est la couche du routage et des adresses.
Elle décide par où passent les paquets pour atteindre la bonne machine dans le monde.

Image simple :

C’est le GPS du réseau.
Elle lit l’adresse du destinataire (IP) et choisit le meilleur itinéraire pour l’atteindre.

Protocoles clés :

- IP (Internet Protocol) : attribue une adresse unique à chaque appareil (IPv4 ou IPv6).
- ICMP : messages de contrôle (utilisés par `ping` pour tester la connectivité).

En OSINT :

C’est la couche où tu cartographies Internet :

- Adresses IP publiques.
- ASN (fournisseurs de blocs d’adresses).
- Traceroutes, géolocalisations, historique DNS.

Exemples d’outils : `whois`, `ipinfo.io`, `bgp.he.net`, `traceroute`, Maltego.

Couche 1 : Accès réseau

(Regroupe les couches 1 et 2 du modèle OSI)

Rôle :

C’est la couche matérielle : les câbles, les antennes, les ondes Wi-Fi, les routeurs.
Elle transforme les données en signaux électriques, lumineux ou radio pour les transporter physiquement.

Image simple :

C’est la route et les véhicules.
Sans elle, aucune donnée ne quitte ton ordinateur.

Protocoles clés :

- Ethernet, Wi-Fi, PPP, ARP, etc.
- Tout ce qui gère le lien direct entre deux machines.

En OSINT :

- Peu exploitable directement, sauf si tu étudies l’infrastructure physique (ex : data centers, câbles sous-marins, antennes).
- Elle t’aide à comprendre la dépendance matérielle d’un pays ou d’un opérateur.

Ressource utile : Submarine Cable Map

Récapitulatif global:

Couche TCP/IP	Correspondance OSI	Rôle simplifié	Exemple de protocole	Observation OSINT
Application	5–7	Dialogue avec l'utilisateur	HTTP, HTTPS, DNS	Headers, contenus, certificats
Transport	4	Acheminement fiable	TCP, UDP	Ports ouverts, services exposés
Internet	3	Adressage et routage	IP, ICMP	IP, ASN, traceroute, whois
Accès réseau	1–2	Transmission physique	Ethernet, Wi-Fi	Infrastructures, câbles, routeurs

💡 Résumé:

Le modèle OSI, c'est la carte : elle t'explique tous les étages et te permet d'être plus précis lorsque tu échanges avec d'autres professionnels.
Le modèle TCP/IP, c'est le manuel de la vraie voiture : il garde juste ce dont on se sert vraiment pour rouler.
Ensemble, ils disent la même chose : comment deux machines, n'importe où sur Terre, peuvent se parler sans se connaître.

4. Une analogie pour ne plus jamais confondre

Imagine que tu veux envoyer un colis à quelqu'un dans un autre pays.
Voici comment les couches se traduisent :

Étape réelle	Équivalent réseau	Couche concernée
Tu écris ton message	Donnée	Application
Tu le mets dans une enveloppe	Encapsulation TCP	Transport
Tu écris l'adresse du destinataire	IP source/destination	Réseau
Le facteur trie et envoie ton courrier	Routage des paquets	Réseau
Le camion l'achemine sur la route	Support physique	Accès réseau
Le destinataire ouvre la lettre	Décapsulation	Application

Cette analogie (colis postal) est utilisée partout en cybersécurité : elle traduit parfaitement le fonctionnement des paquets.

5. Pourquoi cette structure est indispensable

Sans ce découpage :

- chaque fabricant d'ordinateur aurait son propre système de communication ;
- un iPhone ne pourrait pas parler à un PC ;
- un navigateur ne pourrait pas accéder à un serveur d'un autre continent.

Grâce aux couches :

- tout le monde parle la même langue (protocole IP),
- les échanges sont segmentés, testables et indépendants,
- et un problème peut être localisé précisément ("couche réseau", "couche transport", etc.).

Pour l'analyste OSINT : comprendre ces couches permet de situer les empreintes techniques :

- adresse IP (couche 3),
- port ouvert (couche 4),
- service en écoute (couche 7).

6. Comment les couches coopèrent

Prenons un exemple concret : tu tapes dans ton navigateur :

https://example.com

Ton ordinateur :

1. Couches 7 à 5 (Application) → envoie une requête HTTP "GET /".
2. Couche 4 (Transport) → TCP divise la requête en paquets.
3. Couche 3 (Réseau) → IP indique où aller (adresse du serveur).
4. Couches 1–2 (Physique/Liaison) → les bits partent dans les câbles.

À l'arrivée, le serveur fait le trajet inverse pour te renvoyer la page.

Ce va-et-vient constant s'appelle l'échange client-serveur.

7. Les “empreintes” laissées dans chaque couche

Chaque couche laisse des traces qu’un analyste OSINT peut lire.

Couche	Exemple d’empreinte	Outils OSINT concernés
1–2	Type de connexion, adresse MAC (locale), Wi-Fi	Wireshark (local)
3	Adresse IP, ASN, géolocalisation	WHOIS, ipinfo.io, Maltego
4	Ports ouverts, services exposés	Shodan, Nmap
5–7	Protocoles utilisés, certificats, headers HTTP	curl, Wappalyzer, BuiltWith

Ces traces ne nécessitent aucune intrusion : elles sont visibles publiquement et exploitables légalement.

8. Résumé

“Internet est comme un immeuble de 7 étages où chaque niveau fait un travail précis.
Le modèle OSI te montre comment tout est organisé,
le modèle TCP/IP t’explique comment c’est réellement construit.
Ton navigateur vit au dernier étage, ton câble Ethernet au rez-de-chaussée,
et entre les deux, tes données voyagent dans des enveloppes protocolaires.”

9. Mini-exercice : “Range les couches”

Associe chaque élément à sa couche principale (fais le pour le modèle OSI et pour le modèle TCP/IP) :

- HTTP
- TCP
- IP
- Ethernet
- DNS
- ICMP

La correction est sur la page suivante !

Correction :

Pour modèle OSI:

Élément	Couche attendue
HTTP	Application (couche 7)
TCP	Transport (couche 4)
IP	Réseau (couche 3)
Ethernet	Liaison / Physique (couches 2 et 1)
DNS	Application (couche 7
ICMP	Réseau (couche3)

Pour modèle TCP/IP:

Élément	Couche attendue
HTTP	Application (couche 4)
TCP	Transport (couche 3)
IP	Internet (couche 2)
Ethernet	Accès réseau (couche 1)
DNS	Application (couche 4)
ICMP	Internet (couche 2)

Vérifie-toi : si tu peux replacer ces 6 éléments, tu maîtrises déjà la logique réseau.
Félicitations !

10. Ce qu’il faut retenir

Notion	Résumé clair
Modèle OSI	7 couches pour comprendre comment circulent les données.
Modèle TCP/IP	Version simplifiée utilisée réellement sur Internet.
Encapsulation	Chaque couche ajoute sa propre “enveloppe” avant envoi.
Décapsulation	Le destinataire retire les enveloppes une à une.
OSINT & couches	Les outils OSINT exploitent principalement les couches 3 à 7.

11. À ce stade, tu dois savoir :

- Expliquer la logique des couches réseau.
- Distinguer OSI (théorique) et TCP/IP (pratique).
- Comprendre le concept d’encapsulation et de trajet client-serveur.
- Situer où agissent les outils OSINT (WHOIS, Shodan, Maltego, etc.).

Chapitre 4 : Ce qu’un analyste OSINT doit comprendre des couches (Pratique : couches 1–3 et 4–7)

1) Rappel rapide — pourquoi ça nous concerne

Chaque couche du réseau laisse des traces exploitables. Pour un analyste, il faut savoir :

- *repérer* ces traces,
- *interpréter* ce qu’elles signifient pour la cible,
- *savoir quelles limites* elles ont (CDN, NAT, proxys).

On passe ici des éléments basiques (IP, ASN, whois) aux éléments applicatifs (headers, certificats, métadonnées).

PARTIE A - Couches 1 à 3 : physique, liaison, réseau (IP, routage, ASN)

A.1 Adresses IP — ce qu'elles disent (et ce qu'elles cachent)

- IP publique = point d'accès visible sur Internet. Elles identifient *un* endpoint réseau, pas une personne.
- IPv4 vs IPv6 : mêmes usages ; IPv6 est plus long et moins compressé dans certains outils.
- IP privée / NAT : une IP privée (192.168.x.x, 10.x.x.x) n'est pas routable sur Internet (attention aux faux positifs.)

Commandes utiles sur Terminale :

- `ping example.com` → obtenir une IP (rapid check).
- `dig +short example.com` → résolution DNS A/AAAA.
- `whois 93.184.216.34` → propriétaire du bloc IP.

Interprétation:

- IP → rechercher ASN, plage, propriétaire (`whois`, `bgp.he.net`, `ipinfo.io`).
- Une IP dans un range AWS/OVH/Hetzner signale souvent un hébergement cloud ; pas nécessairement le propriétaire final.

Pièges:

- CDN / reverse proxy : IP peut appartenir à Cloudflare/Akamai → ce n'est pas l'origine.
- Shared hosting : une IP peut héberger des centaines de domaines.

A.2 ASN, BGP et routage — la carte des fournisseurs

- ASN (Autonomous System Number) : groupe d'IP géré par un opérateur. Permet de comprendre *chez qui* est hébergée l'infra à l'échelle opérateur.
- BGP : protocole d'échange entre ASN → tracer les chemins inter-opérateurs.

Outils

- `bgp.he.net/AS<number>` pour explorer ASN.
- `whois --verbose IP` ou `ipinfo.io/IP` pour obtenir ASN + organisation.
- `traceroute example.com` / `mtr` pour voir les hops (chaîne de routage).

Interprétation pratique

- Plusieurs cibles partageant le même ASN → possibilité de corrélation (même fournisseur).
- Si le traceroute s'arrête ou montre des IP appartenant à Cloudflare → présence de CDN/proxy.

A.3 Reverse DNS, PTR, et historique DNS

- PTR (reverse DNS) : peut donner un nom de machine lié à l'IP (utile mais souvent générique).
- Historique DNS : `crt.sh`, `securitytrails`, `viewdns` pour retrouver anciennes IP/certificats → C'est un moyen de retrouver l'IP d'origine si le CDN actuel masque la cible.

Commandes utiles sur Terminale:

- `dig -x 93.184.216.34 +short` → PTR.
- `crt.sh?q=%.example.com` → certificats publics listant le domaine/subdomains.

Astuce OSINT : la combinaison historique DNS + anciens certificats permet souvent de bypasser une façade CDN de façon légale (en retrouvant une ancienne IP).

PARTIE B - Couches 4 à 7 : transport → application (ports, services, HTTP, TLS, métadonnées)

B.1 Ports & transport (TCP/UDP)

- Port = porte logique d'un service sur une IP (ex. 80=HTTP, 443=HTTPS, 22=SSH).
- TCP/UDP : TCP = connexion fiable (3-way handshake), UDP = sans connexion (DNS, some media).

Outils

- `nmap -Pn -sS IP` → scan ports (local / avec permission) ; attention légalité.
- **Shodan** pour trouver ports/services exposés publiquement sans scanner soi-même.

Interprétation

- Ports ouverts + banner info → souvent identification du service/version (ex: `nginx/1.18`).
- Plusieurs ports typiques ouverts sur une IP cloud → service multi-composant ou panneau d'hébergement partagé.

Piège : le banner grabbing peut être faux (admins modifient bannières) ; croiser avec d'autres sources.

B.2 HTTP/HTTPS — headers, cookies, en-têtes, comportements

- Headers HTTP (Server, X-Powered-By, Set-Cookie, Content-Security-Policy) donnent des infos techniques (tech stack, WAF, plugins).
- Response codes (200, 301, 404, 503) indiquent comportement et configurations (redirects, protections).

Commandes / outils

- `curl -I https://example.com` → voir headers.
- `curl -v` → échange plus complet.
- Outils : Burp, httpie, Wappalyzer, BuiltWith.

Interprétation

- `Server: cloudflare` → CDN/proxy.
- `Set-Cookie` avec nom spécifique → possible CMS (WordPress, Drupal).
- Headers de sécurité absents → mauvaise hygiène.

B.3 TLS / Certificats SSL

- Certificat TLS contient : CN, SAN (liste de domaines), émetteur, dates, parfois infos organisationnelles.
- crt.sh et Censys permettent de lister tous les certificats publics d'un domaine (utile pour découvrir sous-domaines et anciennes IP).

Commandes

- `openssl s_client -connect example.com:443 -servername example.com` → inspecter certificat.
- `crt.sh` pour historique.

Interprétation

- SANs = sous-domaines potentiels.
- Date d'expiration / émetteur = chaîne de confiance et rotation (Let's Encrypt très fréquent chez startups).

B.4 Applications & données (médias, fichiers, métadonnées)

- Files (PDF, images, docx) embarquent souvent des métadonnées (auteur, GPS, logiciel).
- EXIF dans images : appareil, date, coordonnées GPS (si présentes).
- Repos publics (GitHub) -> fuites de clés, info infra.

Outils

- `exiftool image.jpg` → extraire EXIF.
- `strings`, `binwalk` → analyser binaires/doc.
- `SpiderFoot`, `TheHarvester` → collecte large.

Interprétation

- EXIF GPS → preuve potentielle (toujours vérifier plausibilité).
- Document properties → auteur, logiciel, chemins locaux → corréler avec d'autres indices.

Attention légale : manipuler uniquement des fichiers accessibles publiquement et respecter RGPD/lois.

PARTIE C - TABLEAU SYNTHÈSE : couche > trace > outil OSINT

Couche	Trace exploitable	Outils / commandes
1–2 (physique/liaison)	type de réseau local, Wi-Fi SSID (local only)	Wireshark (local), outils matériels
3 (réseau)	IP, ASN, géoloc, PTR	`dig`, `whois`, `ipinfo`, `bgp.he.net`
4 (transport)	ports ouverts, protocoles (tcp/udp)	Shodan, Nmap (avec permission)
5–7 (session, présentation, app)	HTTP headers, cookies, certificats, contenu	`curl`, `openssl s_client`, Wappalyzer, BuiltWith, ExifTool, Maltego, SpiderFoot