



# DIGITAL FORENSICS INVESTIGATION



CYBER CRIME

Réalisé par:  
ZABRATI Hind

Encadré par:  
Mr SADQI Yassine

# Plan

- 1- Introduction**
- 2- Définition du criminalistique numérique**
- 3- Preuve numérique:**
- 4- Objectifs de la criminalistique numérique**
- 5-Processus d'investigation numérique**
- 6-Banches de la criminalistique numérique**
- 7-Outils de la criminalistique numérique**
- 8-Techniques de la criminalistique numérique**
- 9-Conclusion**
- 10-Références**

# Introduction

Avec l'émergence des technologies numériques, les cyber crimes tels que l'espionnage informatique, le phishing et les attaques par ransomware se multiplient. La criminalistique numérique est devenue un domaine clé pour identifier, préserver, analyser et présenter les preuves numériques. Nos appareils numériques, contenant de nombreuses données personnelles, sont des cibles vulnérables aux cyberattaques. Les enquêteurs doivent analyser des systèmes complexes et répondre rapidement aux incidents de sécurité.





# Définition

La criminalistique numérique est un processus d'investigation en cybersécurité, visant à collecter, analyser et présenter des preuves numériques provenant d'ordinateurs, de réseaux ou d'appareils mobiles, dans le but d'enquêter sur des actes criminels ou des incidents de sécurité. Elle permet d'identifier les auteurs, de comprendre les attaques et de garantir la validité juridique des preuves.



# Preuve numérique

Les preuves numériques sont définies comme des informations et des données de valeur pour une enquête qui sont stockés, reçus ou transmis par un appareil électronique. Cette preuve peut être obtenue lorsque des appareils électroniques sont saisis et sécurisés pour examen.



# Caractéristiques des preuves

Pour être acceptées par un tribunal, les preuves numériques doivent être :

- **Recevables** : pertinentes, impartiales et liées à l'affaire.
- **Authentiques** : leur origine et intégrité doivent être vérifiables.
- **Complètes** : elles doivent confirmer ou infirmer les faits en question.
- **Fiables** : obtenues via une méthode rigoureuse, avec une traçabilité complète.
- **Crédibles** : présentées de façon claire, compréhensible et validées par des experts.





# Types des preuves numériques



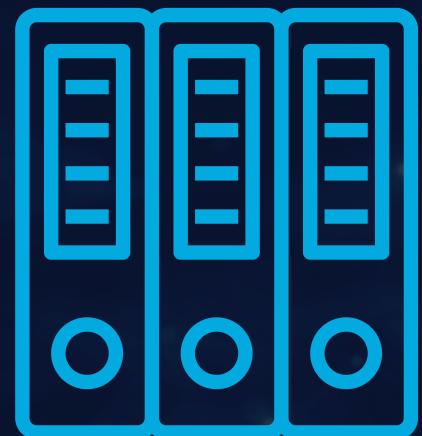
## Fichiers LOG

Historiques des événements sur les systèmes, bases de données ou réseaux (par exemple : connexions, modifications, erreurs, accès non autorisés)



## Images et vidéos

Capturent des preuves visuelles en temps réel (par exemple : caméras de surveillance, photos/vidéos avec métadonnées comme GPS )



## Archives

Fichiers compressés (ZIP, RAR...) contenant des documents, images, bases de données ou codes sources pouvant révéler des intentions ou identités.

# Types des preuves numériques



## Données actives

Fichiers récents ou utilisés en cours de session (par exemple : fichiers temporaires, fichiers de session)



## Métadonnées

Informations intégrées aux fichiers (par exemple : auteur, date de création, emplacement GPS) essentielles pour prouver l'origine et la chronologie des actions.

# Objectifs de la criminalistique numérique

- Analyser les preuves électroniques
- Identifier les responsables et les méthodes utilisées
- Évaluer les dommages causés par l'attaque
- Préparer des preuves recevables en justice
- Renforcer la sécurité en détectant les failles exploitées
- Prévenir de futures attaques en corrigeant les vulnérabilités





# Processus de l'investigation numérique

Désigne le chemin que les preuves numériques suivent depuis leur identification jusqu'à leur présentation devant une autorité judiciaire

Nous suivons ici le modèle proposé par DFRWS (Digital Forensic Research Workshop), structuré en 6 étapes clés pour guider une enquête numérique.



1

2



## Identification

Présente l'étape initiale et l'une des plus critiques où l'on détecte un incident et identifie les sources de preuves numériques qui peuvent être des ordinateurs, serveurs, téléphones, tablettes ou supports de stockage externes

► Basée sur le principe d'échange de Locard : toute interaction laisse des traces.

## Préservation

Une fois les preuves identifiées, il est important de les protéger contre toute modification ou suppression.

- Interdire l'accès au système suspect aux utilisateurs.
- Isolement du système du reste du réseau par des contrôles d'accès.
- Capture instantanée et sauvegarde sur un stockage non volatile.

3



### Collecte

Elle consiste à recueillir, de manière rigoureuse et documentée, toutes les données pertinentes identifiées lors de la phase précédente.

- Priorité aux données volatiles (RAM, connexions actives), en respectant la chaîne de conservation.
- Documentation complète obligatoire pour garantir la recevabilité juridique.

4



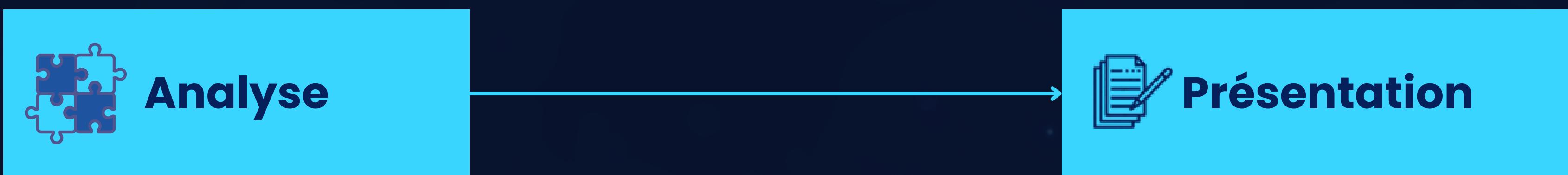
### Examen

Analyse technique et minutieuse des preuves à l'aide d'outils forensiques.

- Recherche d'éléments cachés ou supprimés : fichiers, logs, traces de malware, métadonnées.
- Réalisée sur une copie (image bit-à-bit), pour préserver l'intégrité de l'original.

5

6



Elle consiste à analyser les données pour reconstituer les événements de l'incident, identifier les vulnérabilités, les systèmes affectés et les auteurs de l'intrusion.

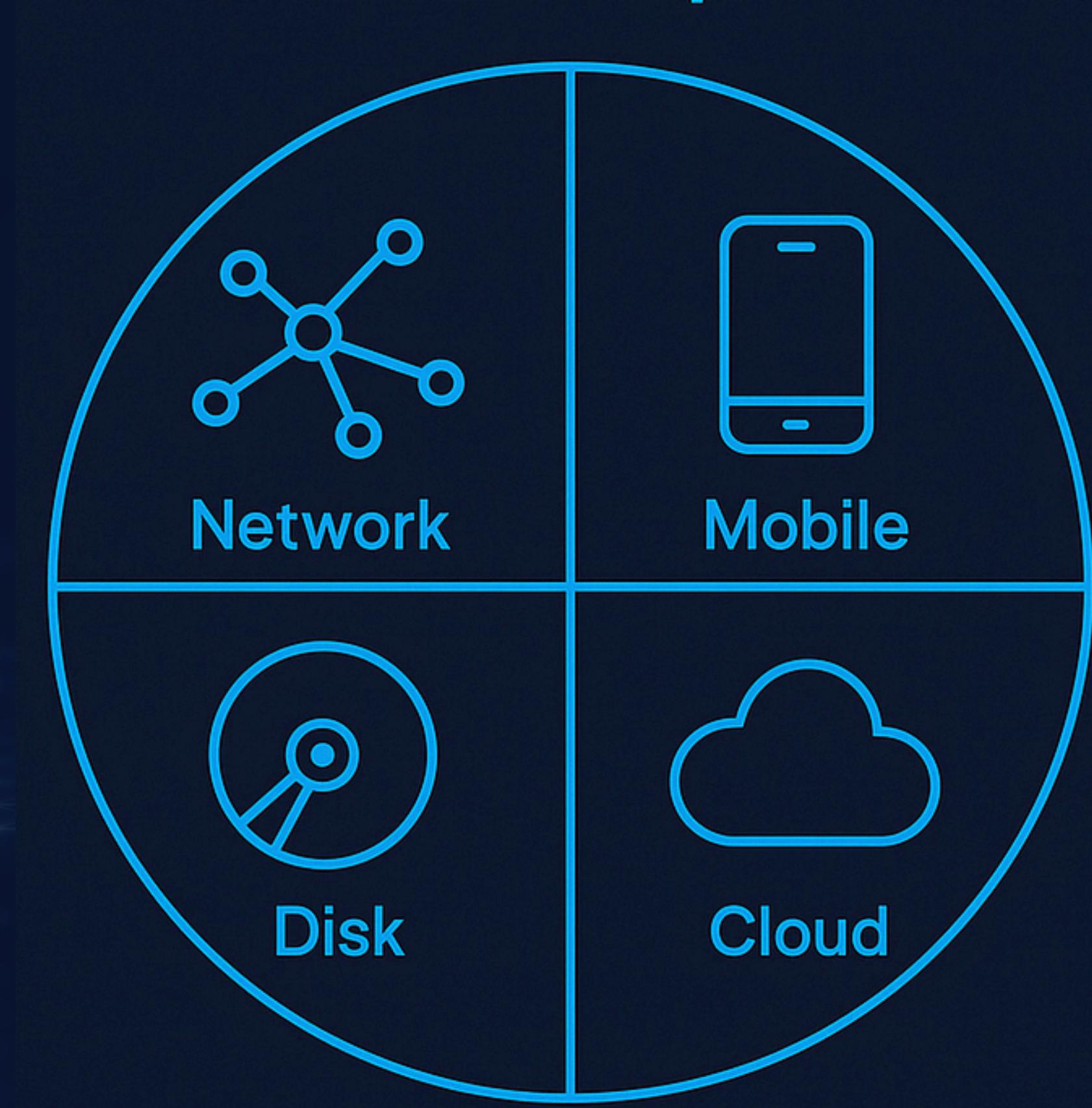
- Corrélation des données entre elles (trafic réseau, logs, menaces connues).
- Vise à reconstituer le scénario de l'attaque.

Finalisation du processus avec la rédaction d'un rapport clair, structuré et impartial.

- Le rapport peut servir devant la direction ou en justice.
- L'expert peut être amené à témoigner comme témoin technique ou expert.

# Branches de la criminalistique numérique

La criminalistique numérique est un vaste domaine englobant diverses sous-disciplines, chacune axée sur un aspect spécifique de la collecte et de l'analyse des preuves numériques. Voici les principales branches de la criminalistique numérique :



## Criminalistique réseau

La criminalistique réseau analyse le trafic pour détecter des intrusions et recueillir des preuves.

Elle repose sur:

- la capture de paquets
- l'analyse des logs des dispositifs réseau
- l'examen des flux de trafic.

Les sources de preuves incluent le trafic réseau, les logs des pare-feu, IDS et applications. Cette discipline aide à comprendre les attaques, identifier les vulnérabilités et améliorer la sécurité du réseau.

## NETWORK



# Criminalistique des appareils mobiles

La criminalistique des appareils mobiles consiste à récupérer des preuves numériques à partir de dispositifs comme les téléphones, tablettes et GPS.

Elle permet d'extraire des données personnelles et professionnelles, telles que:

- l'historique des appels, des messages, des photos, des vidéos
- les informations de géolocalisation.

Les principales méthodes d'acquisition sont manuelle, logique, physique, ou par force brute. Cette discipline est cruciale pour enquêter sur les fraudes, les vols ou d'autres crimes impliquant des appareils mobiles.



## MOBILE FORENSICS



# Criminalistique des supports de stockage

La criminalistique des supports de stockage vise à analyser des dispositifs comme les disques durs et clés USB pour récupérer des données importantes, y compris les fichiers supprimés, les fragments de fichiers, et les métadonnées. Elle est essentielle pour les enquêtes judiciaires et la récupération de données. Les méthodes d'acquisition incluent l'extraction physique, logique et par force brute, et l'analyse de supports comme les cartes mémoire ou les disques externes.

# DISK FORENSICS



# Criminalistique du Cloud

La criminalistique du cloud s'intéresse à l'analyse des données hébergées sur des services distants comme AWS, Azure ou Google Cloud. Elle permet de collecter et préserver des preuves numériques liées à des crimes tels que les violations de données ou vols d'identité. Les preuves varient selon le modèle cloud utilisé (SaaS, PaaS, IaaS) et peuvent inclure des journaux d'accès, des configurations ou des instantanés système. Elle présente des avantages comme l'accessibilité mondiale et l'évolutivité, mais aussi des défis tels que la sécurité des données, la complexité technique et la perte de contrôle sur l'infrastructure.



# Outils de la criminalistique numérique

Les outils de criminalistique numérique servent à collecter et préserver des preuves numériques.

Différentes critères doivent être prise en compte lors du choix des outils :

- Sur quel système d'exploitation l'outil d'investigation fonctionne-t-il?
- Est-il polyvalent?
- Peut-il analyser plusieurs systèmes de fichiers?
- Un langage de script peut-il être utilisé pour automatiser les fonctions et tâches répétitives ?

Ces critères aident à choisir des outils adaptés aux enquêtes, tout en garantissant leur fiabilité et leur validité juridique.



Wireshark



FTK  
IMAGER



Volatility



Autopsy



Andriller



CAINE  
Linux



# Outils de la criminalistique numérique



## Wireshark

Outil gratuit d'analyse du trafic réseau en temps réel. Il permet de détecter les connexions suspectes, les fuites de données et les attaques DoS. Il utilise des filtres, la coloration des paquets, et la résolution DNS pour faciliter l'analyse.



## FTK Imager

Outil d'imagerie forensique permettant d'acquérir, prévisualiser, analyser et récupérer des données sur disques ou périphériques. Il supporte plusieurs formats et offre des fonctions de comparaison, d'export et de génération de rapports.



## Autopsy

Plateforme open source d'investigation numérique avec une interface simple. Elle permet l'analyse de fichiers, d'artefacts web, d'e-mails, de registres et la récupération de données supprimées. Elle génère aussi des rapports judiciaires.

# Outils de la criminalistique numérique



## Volatility

Framework d'analyse forensique de la mémoire vive (RAM). Il extrait les processus actifs, connexions réseau, artefacts système, etc. Très utilisé pour détecter les malwares et reconstituer les événements grâce à des plugins.



## Andiller

Outil spécialisé dans l'analyse forensique des smartphones Android. Il permet l'extraction et le décodage de données, le déverrouillage d'écrans, l'analyse des bases de données d'applications comme WhatsApp, et la génération de rapports.



## CAINE Linux

Distribution Linux complète pour l'investigation numérique, intégrant des outils comme Autopsy, Wireshark, The Sleuth Kit, PhotoRec, etc. Elle fonctionne depuis une clé USB et permet l'analyse mémoire, disque, réseau et système.



# Techniques de la criminalistique numérique

## Stéganographie inversée

Méthode qui détecte les données cachées dans des fichiers (images, vidéos, etc.) en comparant leurs hachages.

## Analyse stochastique

Technique utilisée quand il n'y a pas d'artefacts numériques visibles. Elle permet de déduire une activité suspecte (comme un vol de données) en analysant des comportements irréguliers.

## Analyse en temps réel

Examen d'un appareil pendant qu'il est encore en marche, pour récupérer des données volatiles (RAM, cache, processus en cours).



# Techniques de la criminalistique numérique

## Analyse croisée (CDA)

Technique qui compare les données de plusieurs disques pour identifier des schémas ou éléments communs (emails, identifiants, etc.). Elle permet de repérer des liens cachés entre plusieurs sources.

## Récupération de fichiers supprimés

Aussi appelée "sculpture de fichiers", elle consiste à retrouver des fichiers effacés en analysant les fragments laissés sur le disque.

# Conclusion

La criminalistique numérique joue un rôle crucial pour répondre aux incidents, renforcer la prévention et assurer la traçabilité. Grâce à des preuves objectives, un processus rigoureux d'investigation, des branches spécialisés comme le cloud ou les appareils mobiles, ainsi que des outils adaptés, elle permet d'identifier, d'analyser et de présenter des éléments numériques recevables devant la justice.

Dans un monde de plus en plus connecté, la maîtrise de ces compétences est essentielle pour assurer la sécurité, faire éclater la vérité et défendre la justice.

# Références

- 1. Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, Christopher K. Steuart and Robert S. Wilson**
- 2. Digital Forensics and Incident Response by Gerard Johansen**
- 3. Handbook of Digital Forensics and Investigation edited by Eoghan Casey**
- 4.[https://www.e-spincorp.com/master-network-forensics-tools-techniques-best-practices cybersecurity/](https://www.e-spincorp.com/master-network-forensics-tools-techniques-best-practices-cybersecurity/)**
- 5.[https://en.wikipedia.org/wiki/CAINE\\_Linux](https://en.wikipedia.org/wiki/CAINE_Linux)**
- 6. <https://www.geeksforgeeks.org/techniques-of-cyber-forensics/>**
- 7. <https://zimperium.com/glossary/mobile-device-forensic>**
- 8.<https://www.appdirect.com/blog/cloud-forensics-and-the-digital-crime-scene>**
- 9.<https://translate.google.com/>**

# La manière d'utilisation de l'IA génératives

Dans le cadre de ce projet l'intelligence artificielle générative, en particulier ChatGPT, a été utilisée pour :

- Reformuler et structurer certaines sections théoriques du rapport.
- Expliquer des concepts complexes
- Fournir des suggestions de plans, de transitions logiques entre les parties
- Accompagner l'élaboration de la partie pratique, notamment dans l'installation, le choix de l'image disque...
- Génération d'illustrations à inclure dans le rapport et la présentation pour appuyer visuellement les explications.
- Résumés clairs et structurés des grandes parties du projet pour inclure dans la présentation

J'ai utilisé l'IA comme un assistant intelligent, pour gagner du temps, améliorer la qualité de l'écriture, et faciliter la compréhension de notions techniques.



MERCI POUR VOTRE  
ATTENTION