MINI PROJET
-
BASES DE DONNÉES

RAPPORT

MODÉLISATION D'UNE BASE DE DONNÉES POUR LES ENQUÊTES JUDICIAIRES NUMERIQUES

Membres du groupe :
AGNIMEL Kelel
GUE Blé Manuela

Professeur :
Lena TREBAUL

ING 1 - NEW 1

ble.gue@efrei.net
kelel.agnimel@efrei.net

Dans le cadre du mini-projet du cours de bases de données, nous avons décidé de travailler dans le domaine de la CRIMINALITE en faisait **la conception d'un système d'information**. Pour cela nous avons utilisé l'IA générative en lui envoyant notre prompt qui utilise le Framework RICARDO.

Voici les résultats obtenus :

I- Les règles métier

• Chaque dossier d'enquête doit avoir un numéro unique généré automatiquement, associé à un type d'infraction spécifique comme cyberfraude, trafic de drogue en ligne ou blanchiment via cryptomonnaies, et un état actuel (ouvert, en cours, clos).

• Les personnes impliquées, qu'il s'agisse de suspects, témoins, victimes ou informateurs, doivent être enregistrées avec des identifiants uniques et des niveaux de confidentialité pour protéger les sources sensibles.

• Les acteurs externes tels que banques, agences partenaires internationales, avocats ou tribunaux doivent être listés avec des contacts vérifiés et des accords de collaboration pour faciliter les échanges d'informations.

• Les preuves matérielles ou numériques, comme des dispositifs saisis ou des logs informatiques, doivent être cataloguées avec une description détaillée et une chaîne de garde ininterrompue pour garantir leur admissibilité en justice.

• Les flux financiers suspects, incluant comptes bancaires, transactions en ligne ou valeurs saisies, doivent être tracés avec des montants précis et des origines vérifiées pour détecter les schémas de blanchiment.

• Toute opération sur le terrain, telle qu'une perquisition numérique, une saisie de serveurs ou une arrestation, doit être documentée avec des dates, heures et participants pour assurer la traçabilité.

• Les documents judiciaires, comme mandats d'arrêt ou décisions de tribunal, doivent être stockés avec des références croisées aux dossiers pour accélérer les procédures légales.

• Les fichiers médias, incluant photos de scènes de crime virtuelles, vidéos de surveillance en ligne ou enregistrements audio de communications interceptées, doivent être étiquetés avec des métadonnées pour authentification.

• Les localisations et chronologies des événements, y compris adresses IP, coordonnées GPS ou timelines d'attaques cyber, doivent être enregistrées précisément pour reconstruire les séquences d'activités criminelles.

• La chaîne de garde pour toutes les preuves doit inclure une liste chronologique des personnes qui y ont accédé, avec dates et raisons, pour éviter toute contestation.
• Les métadonnées d'accès aux données sensibles doivent logger qui a consulté ou édité quoi, quand et depuis quel appareil, pour détecter les fuites potentielles.

• Les informateurs confidentiels doivent avoir un statut protégé, avec des règles strictes limitant l'accès à leurs informations à un petit nombre d'agents autorisés.

• Les transactions financières liées à la cybercriminalité, comme des paiements en bitcoin, doivent être analysées pour des patterns récurrents et liées à des suspects.

• Toute collaboration avec des agences externes doit être approuvée au préalable et documentée pour respecter les protocoles internationaux.

• Les dossiers clos doivent être archivés après un délai de 5 ans, mais restent accessibles pour réouverture en cas de nouveaux éléments.

• Les victimes de cybercriminalité doivent être notifiées des avancées de l'enquête si elles en font la demande, avec des mesures de protection de leur identité.

• Les biens saisis, qu'ils soient physiques (ordinateurs) ou virtuels (comptes gelés), doivent être évalués et stockés avec des rapports d'expertise.

II- Le dictionnaire de données

Signification de la donnée	Type	Taille
Numéro de dossier	VARCHAR	20
Type d'infraction	VARCHAR	50
Etat du dossier	VARCHAR	20
ID de la personne	VARCHAR	15
Nom de la personne	VARCHAR	100
Date de naissance de la personne	DATE	10 (YYYY-MM-DD)

Adresse IP de la personne	VARCHAR	45
Rôle de la personne	VARCHAR	30
Témoignage de la personne	CHAR	5000
Adresse email de la personne	VARCHAR	100
Nom de la banque impliquée	VARCHAR	100
Nom de l'agence partenaire	VARCHAR	100
Nom de l'avocat	VARCHAR	100
Nom du tribunal	VARCHAR	100
Description de la preuve	VARCHAR	500
Type de bien saisi	VARCHAR	50
Numéro de compte bancaire	VARCHAR	20
Montant de la transaction	DECIMAL	15
Valeur saisie	DECIMAL	15
Date et heure de perquisition	DATETIME	19(YYYY-MM-DD / HH: MM: SS)
Lieu d'arrestation	VARCHAR	200
Numéro de mandat judiciaire	VARCHAR	15
Decision de justice	CHAR	1000
Nom du fichier media	VARCHAR	255
Type de media (photo/vidéo)	VARCHAR	20
Coordonnées GPS	VARCHAR	50
Date de l'évènement	DATE	10
Heure de l'évènement	TIME	8 (HH :MM : SS)
Nom de l'agent responsable de la chaine de garde	VARCHAR	100
Date d'accès aux données	DATETIME	19
Utilisateur qui a édité	VARCHAR	50
Type de malware détecté	VARCHAR	50
Log d'activité cyber	CHAR	10000
Montant en cryptomonnaie	DECIMAL	15