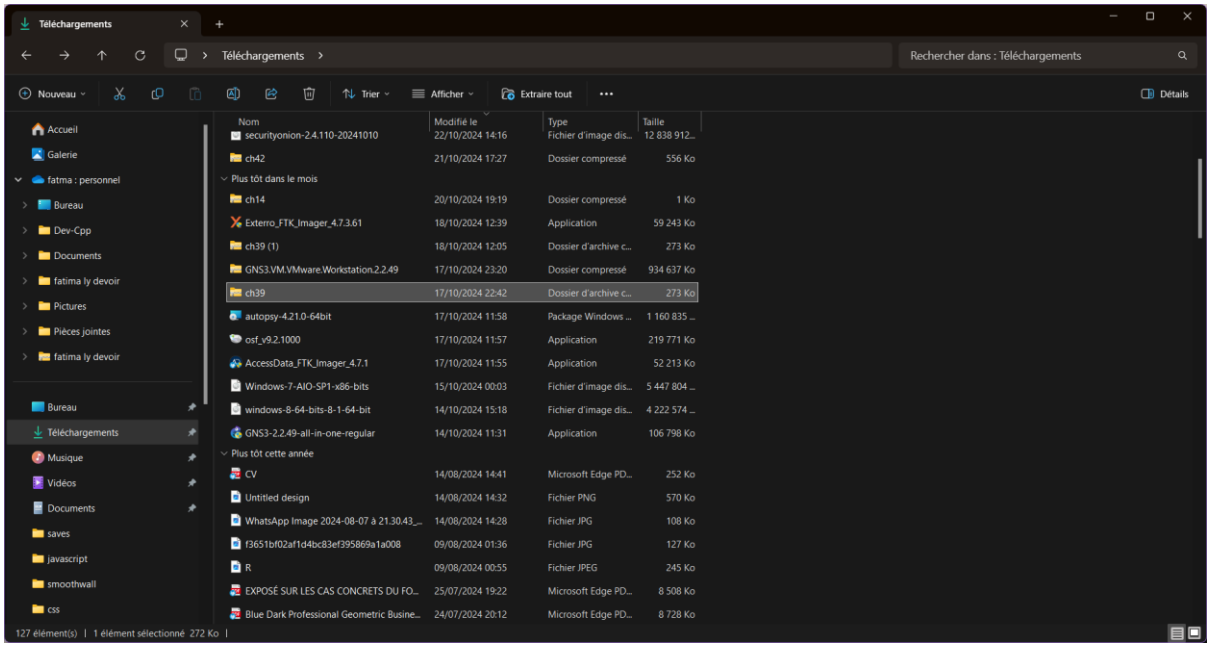
EXERCICE de rapport

Exercice :

Une entreprise soupçonne qu'un de ses employés à exporter des données confidentielles sur des concourants en utilisant des moyennes numériques. Vous êtes appelée pour enquêter sur ce soupçon

1. IDENTIFICATION DES PREUVES

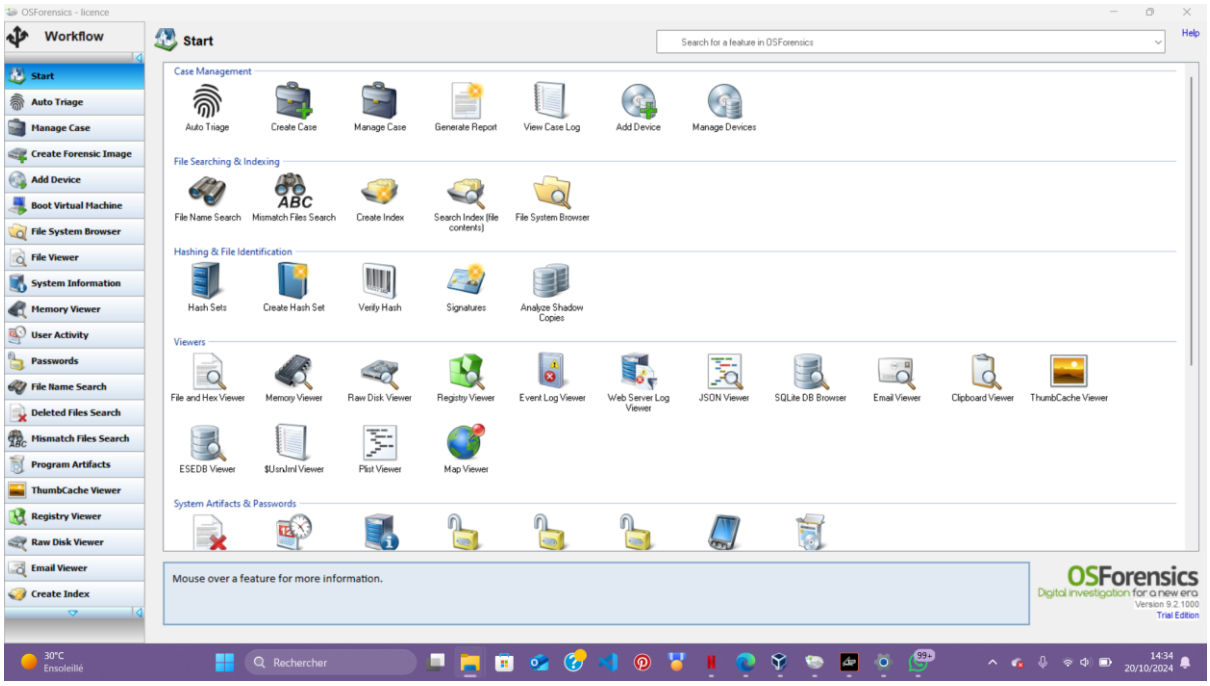
- **Isoler l'environnement concerné :** Si possible, isolez les appareils utilisés par l'employé soupçonné (ordinateur, téléphone portable, etc.) pour éviter toute altération des preuves.
- Créer une copie forensique des disques durs et des autres supports de stockage



- ❖ Nous avons ici une clé USB d'un employé soupçonné pour éviter toute altération, nous allons d'abord faire la copie de la clé USB pour prouver des preuves et tracer les fichiers supprimés

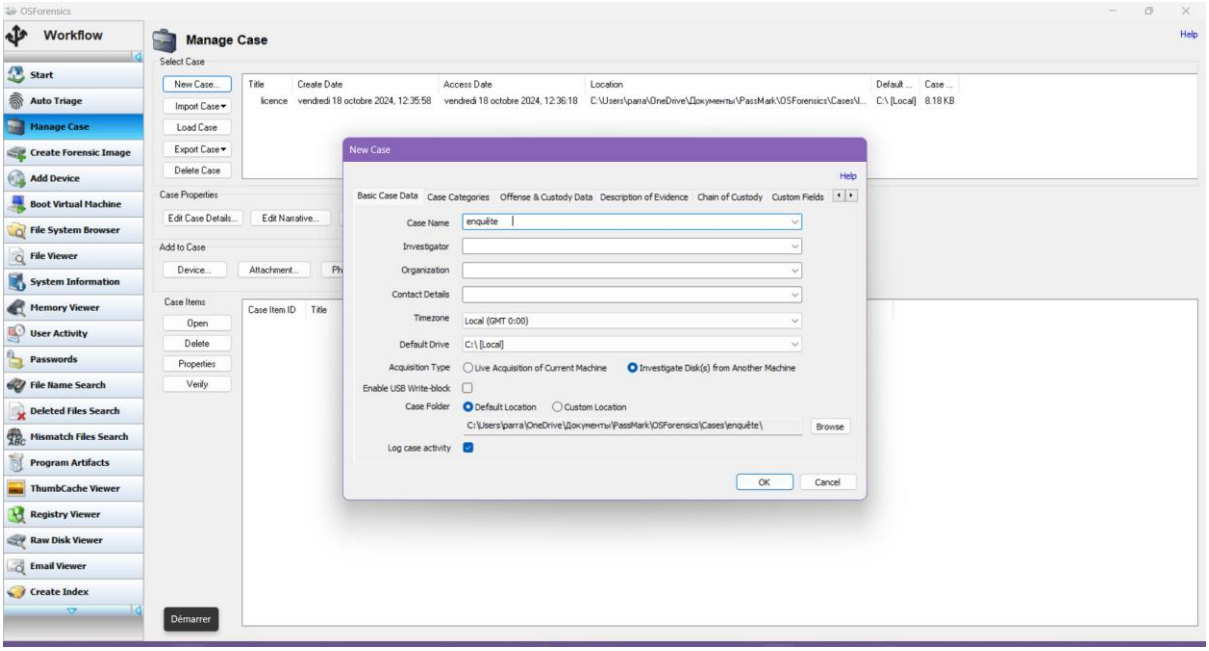
2. Analyse des systèmes

- **Traçage des activités réseau :** Analysez le trafic réseau pour voir si des fichiers ont été transférés vers des plateformes externes (via FTP, email, services de cloud tels que Google Drive, Dropbox, etc.).
- **Analyse des fichiers téléchargés ou copiés :** Utilisez des outils de suivi pour identifier si des fichiers ont été copiés sur des périphériques de stockage externes (clé USB, disque dur externe)

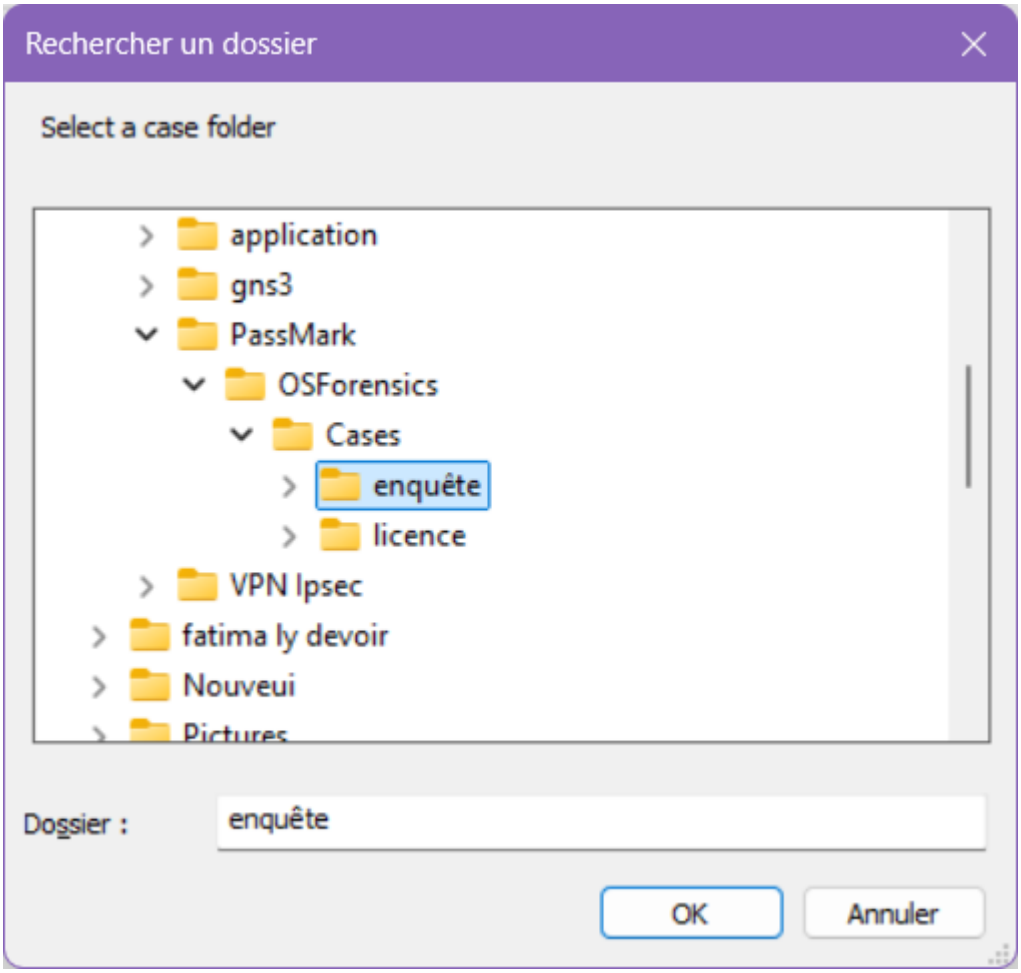


* ensuite pour faire une bonne analyse du système nous allons avoir besoin de OSFORENSIS pour faire la documentation mais aussi Analysez le trafic réseau pour voir si des fichiers ont été transférés vers des plateformes externes (via FTP, email, services de cloud tels que Google Drive, Dropbox, etc.).

- Pour procéder à cette analyse nous allons d'abord Create case c'est à dire donner un nom au fichier si dessous

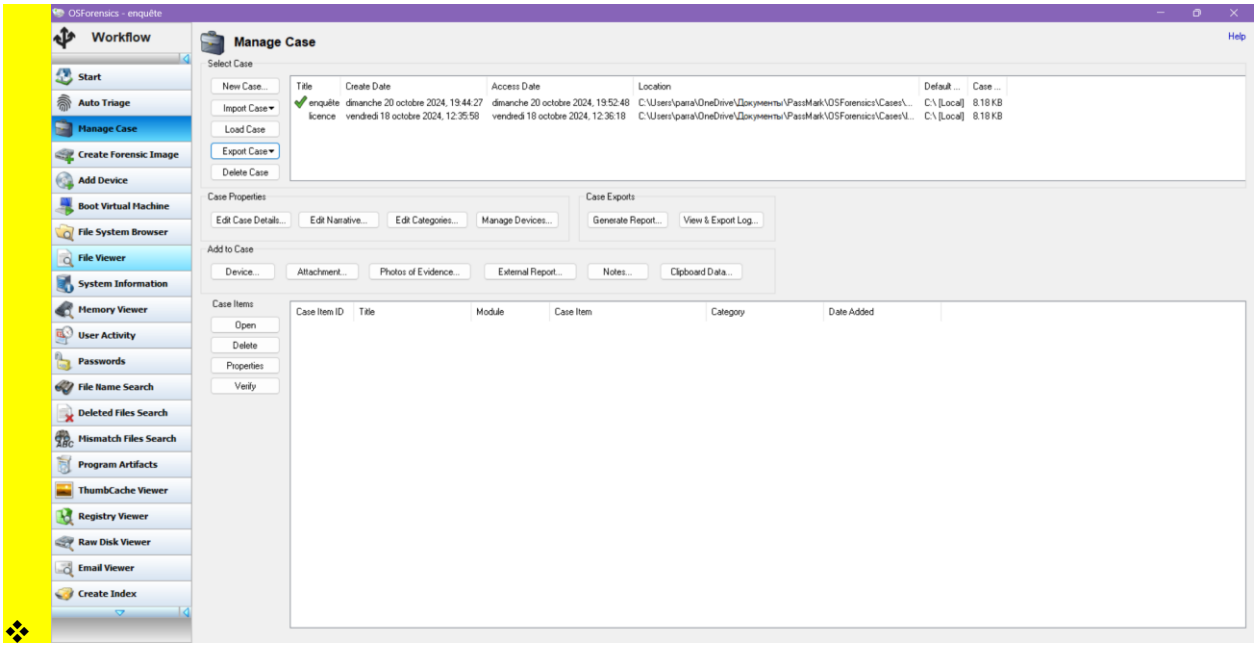


❖ * Après avoir donné au nom au cas, va falloir importer le fichier depuis le répertoire

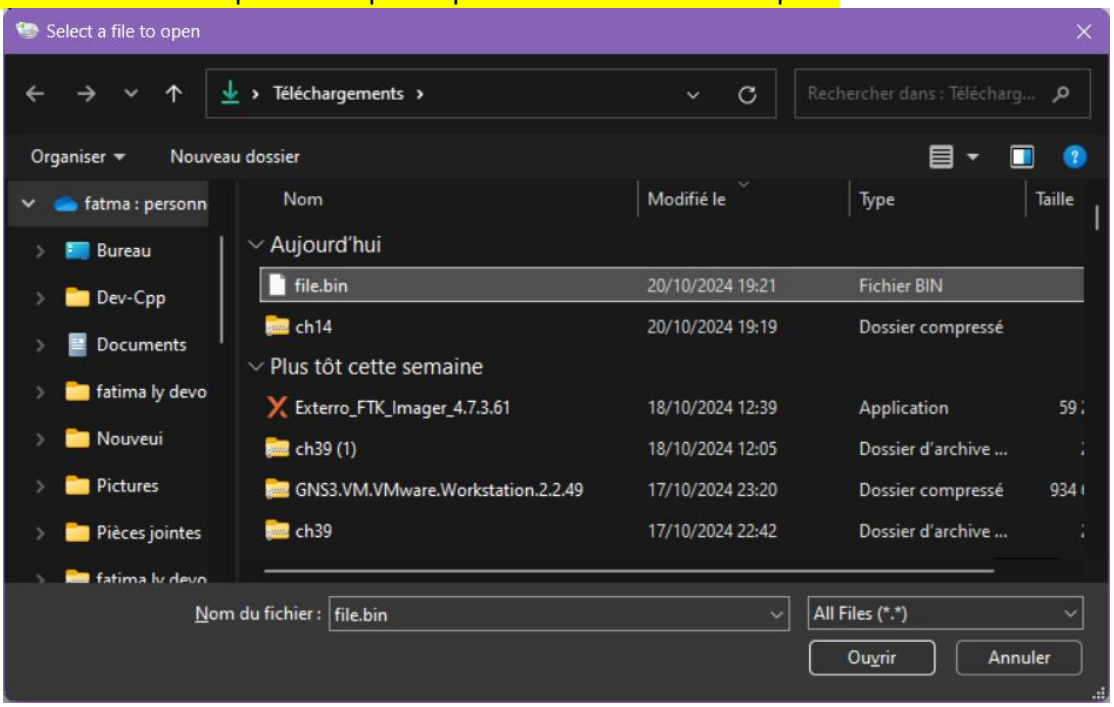


❖

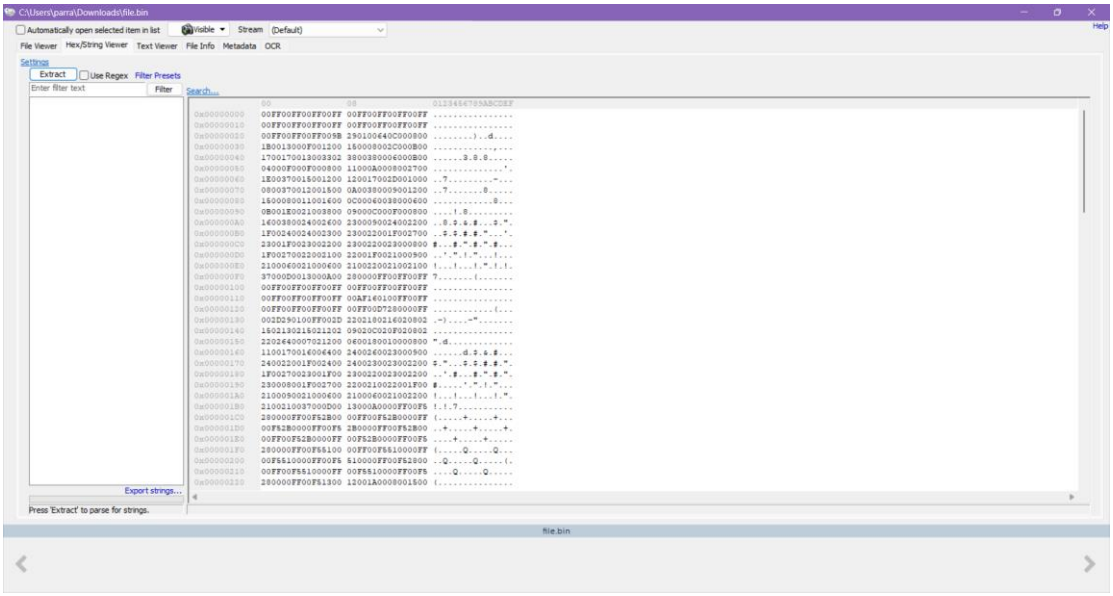
❖ Une fois dans le répertoire il faut sélectionné le nom que nous avons donné au cas et on le sélectionne



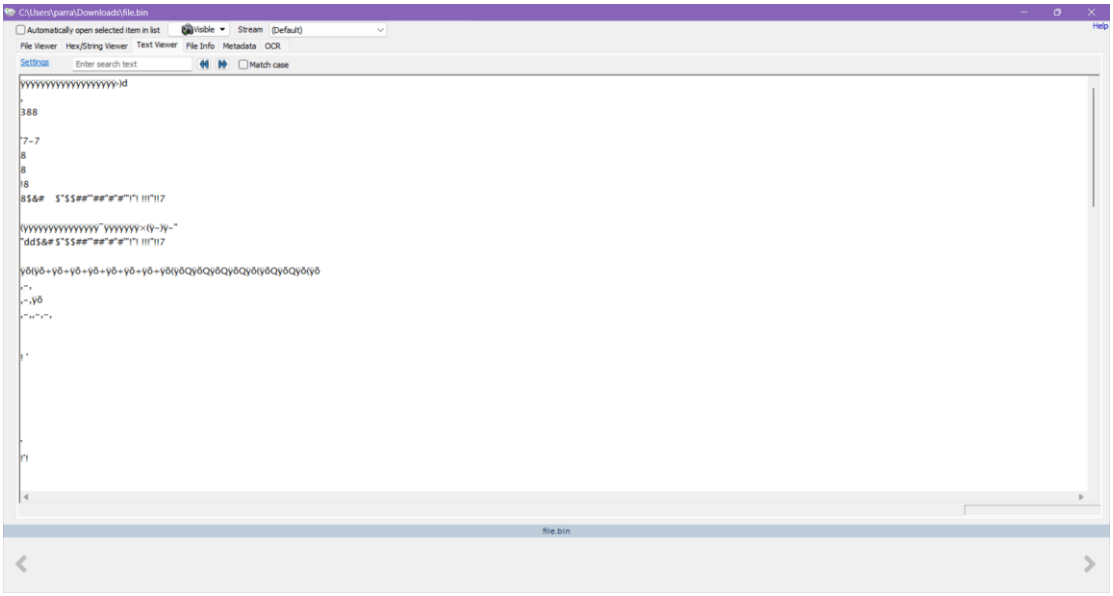
Sur cette image si dessus nous allons partir sur fil viewer pour pouvoir regarder ce qui se trouver dans la clé USB qu'on a copié depuis l'ordinateur du suspect



- On sélectionne l'image du fichier depuis la clé USB pour y accéder



- Voilà un aperçu du déchiffrement de la clé USB c’est à dire ce qu’on a extrait du fichier



Nous avons réussi à décoder la clé contenant un fichier binaire a été retrouvée sur le bureau du stagiaire

3. **Rapport et recommandations**

- **Établissez un rapport détaillé** des conclusions, incluant les dates, les activités, les preuves récupérées et les conclusions concernant la potentielle fuite Action, observation et décision prise au cours de l’investigation a été scrupuleusement documentée en vue de la préparation d’un rapport final qui pourra également servir à l’éventuelle suite judiciaire.

Date : 18/11/24
*Auteur(s) : Fatma Ly
Titre : Analyse forensique sur une fuite potentielle de données confidentielles

1-Sommaire

2- Résumé

Ce rapport détaille une enquête sur un incident potentiel de fuite de données sensibles impliquant un employé. L'objectif principal était de déterminer si cet employé avait transféré des fichiers critiques vers une source non autorisée. Les investigations ont permis de mettre en évidence :
- Des accès inhabituels à des fichiers sensibles.
- Le transfert de données via un service tiers.
- Une utilisation suspecte d'une clé USB.
Ces découvertes soulèvent des inquiétudes concernant la sécurité des données au sein de l'entreprise et mettent en avant la nécessité de renforcer les protocoles existants.

19/11/24 : Détection des premières anomalies dans les accès.
19/11/24 : Isolation de l'environnement suspect et collecte des preuves.
20/11/24 : Analyse approfondie des journaux et des périphériques connectés.

3- Détails des Investigations
Étape 1 : Collecte et préservation des preuves
- L'ordinateur et les périphériques de l'employé suspect ont été isolés immédiatement.
- Une copie forensique des supports (disques durs et clés USB) a été réalisée pour garantir l'intégrité des données
Étape 2 : Analyse des systèmes et activités
- Inspection des fichiers : Certains fichiers sensibles ont été copiés sur une clé USB connectée le 20/11/24 .
- Recherche d'outils suspects : Aucune application malveillante n'a été détectée, mais un logiciel FTP utilisé pour des transferts a été identifié.
Étape 3 : Documentation des actions menées Chaque étape a été soigneusement répertoriée avec des preuves visuelles (captures d'écran, logs réseau) pour garantir la traçabilité de l'analyse.

4-Hypothèses d'Analyse

Jeu de l'analyse : assurer le traitement des pistes selon leur crédibilité, en tenant compte des décisions passées prises (ou non), avec pour conséquence des doutes variables.

La confrontation des résultats avec le vécu des acteurs leur confère une force probante et utilise la synchronisation des faits soulevés.

La consultation des fichiers : Les fichiers accédés par l'employé dans ses temps de travail n'a pas été fourni, ni la justification.

Les accès aux fichiers du disque dur interne du salarié ne sont pas reproduits mais affichent une construction non conventionnelle ; le lecteur USB externe est non protégé et accessible avec une simple clé USB même à distance.

5. Recommandations

La prise de conscience de l'urgence et des enjeux sensibles face à l'ampleur de l'incident a soulevé une alerte. Afin d'améliorer le processus de gestion des dispositifs de sécurité dans l'entrepreneur, il conviendrait de renforcer la conscience professionnelle des salariés notamment en matière :

- D'évaluation des risques,

- De lutte contre la fraude,

- De gestion des comportements suspects, notamment dans les ressources humaines.

6. Liste des Indicateurs de Compromission

Les anomalies de connexions peuvent correspondre à des transferts de fichiers ou à une connexion à leur dommage d'accès non sécurisé dans le cadre de la réutilisation possible illégale des données.

L'observation conclut que l'analyse de chaque de l'auteur des transferts posée risque de compromettre les systèmes d'accès dans les limites d'une possibilité d'atteinte à la cohérence interne des fichiers sensibles. Les cas de lenteur du transfert peuvent être mis en relation avec la découverte d'informations signalant d'un volet ou contenu sensible pouvant nuire à leurs usages loin d'une recherche raisonnable.