Manuel Très Complet de FTK Imager

Introduction : FTK Imager, l'Outil Indispensable de la Criminalistique Numérique

Dans le domaine de la criminalistique numérique (forensics), l'acquisition de données est une étape fondamentale et critique. Pour qu'une preuve numérique soit recevable et fiable, elle doit être collectée de manière intègre, sans altération et en respectant des procédures strictes. C'est dans ce contexte que **FTK Imager** se positionne comme un outil gratuit et puissant, largement reconnu et utilisé par les enquêteurs, les analystes forensiques et les professionnels de la cybersécurité.

Qu'est-ce que FTK Imager ?

FTK Imager est un utilitaire logiciel développé par AccessData (désormais Exterro) qui permet de créer des images forensiques bit-à-bit de disques durs, de clés USB, de la mémoire vive (RAM), de dossiers spécifiques ou même de fichiers individuels. Une image forensique est une copie exacte et fidèle d'un support de stockage, incluant non seulement les fichiers visibles, mais aussi les données supprimées, les espaces non alloués et les métadonnées, le tout sans altérer la source originale.

Pourquoi FTK Imager est-il Essentiel en Criminalistique Numérique ?

FTK Imager est un pilier de la boîte à outils forensique pour plusieurs raisons :

- **Intégrité des Preuves** : L'outil garantit que l'acquisition des données est réalisée de manière

Installation de FTK Imager : Un Guide Détaillé

L'installation de FTK Imager est un processus simple et direct, mais il est important de suivre les étapes pour s'assurer que l'outil est correctement configuré et prêt à l'emploi. FTK Imager est un logiciel Windows, donc ces instructions sont spécifiques à cet environnement.

1. Téléchargement de FTK Imager

FTK Imager est disponible gratuitement sur le site officiel d'Exterro (anciennement AccessData).

1. **Accédez au Site Officiel d'Exterro** : Ouvrez votre navigateur web et naviguez vers la page de téléchargement de FTK Imager : https://www.exterro.com/ftk-imager
2. **Enregistrez-vous ou Connectez-vous** : Exterro exige généralement une inscription gratuite pour télécharger ses outils. Remplissez le formulaire avec vos informations (nom, adresse e-mail professionnelle, organisation, etc.) ou connectez-vous si vous avez déjà un compte.
3. **Téléchargez la Dernière Version** : Une fois le formulaire soumis, vous devriez être redirigé vers la page de téléchargement. Cliquez sur le lien pour télécharger la dernière version de FTK Imager (généralement un fichier `.exe`).

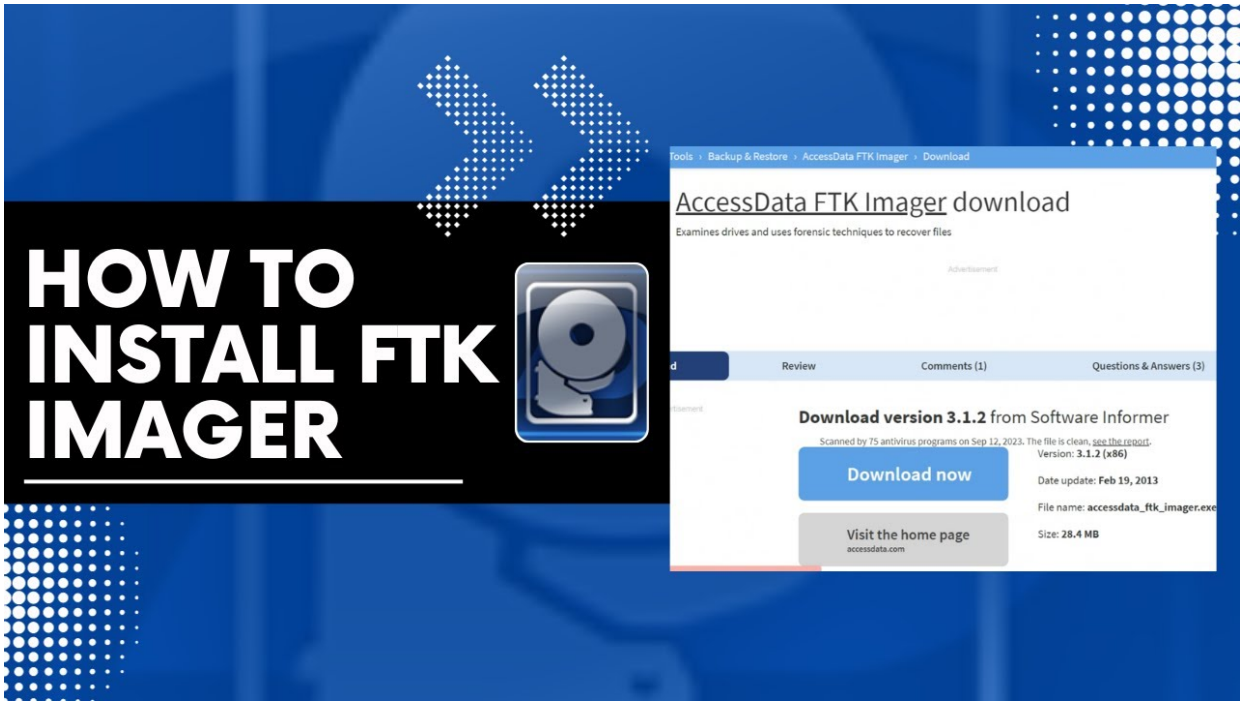

Figure 1: Page de téléchargement de FTK Imager sur le site d'Exterro.

2. Installation de FTK Imager

Une fois le fichier d'installation téléchargé, vous pouvez procéder à l'installation.

1. **Exécutez l'Installeur** : Localisez le fichier `.exe` téléchargé (par exemple, `FTKImager_X.X.X.exe`) et double-cliquez dessus pour lancer l'assistant d'installation.

2. **Assistant d'Installation** :

   - **Écran de Bienvenue** : Cliquez sur `Next` (Suivant) sur l'écran de bienvenue de l'assistant d'installation.
   - **Contrat de Licence** : Lisez attentivement le contrat de licence utilisateur final (EULA). Si vous acceptez les termes, sélectionnez `I accept the terms in the License Agreement` et cliquez sur `Next`.
   - **Dossier de Destination** : Choisissez le dossier où FTK Imager sera installé. Le chemin par défaut est généralement recommandé, sauf si vous avez une raison spécifique de le modifier. Cliquez sur `Next`.
   - **Prêt à Installer** : L'assistant est maintenant prêt à installer le programme. Cliquez sur `Install` (Installer) pour commencer le processus.

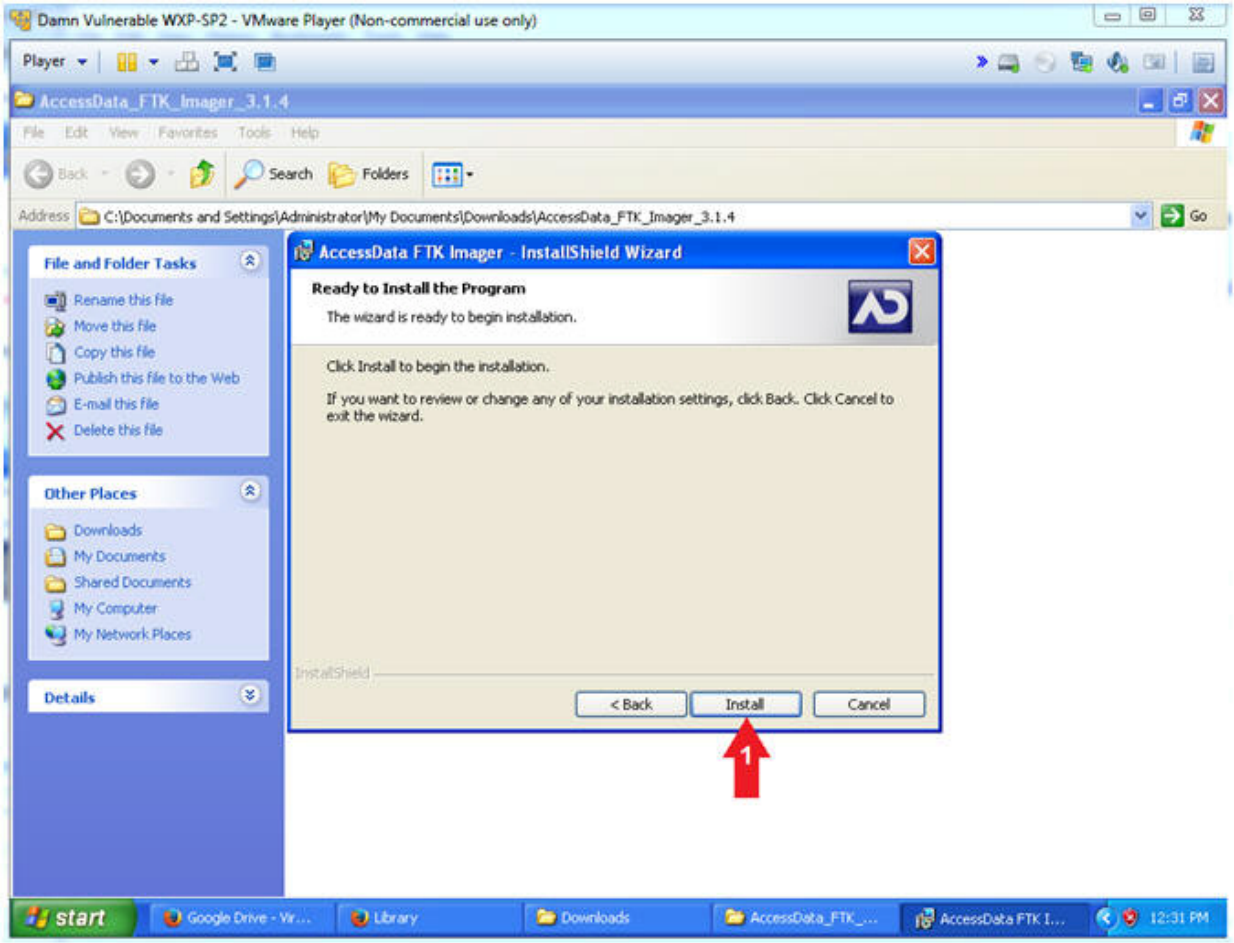

*Figure 2: Assistant d'installation de FTK Imager, montrant l'étape

Création d'une Image Disque avec FTK Imager

La fonction principale de FTK Imager est de créer des images forensiques de divers supports de stockage. Ce processus est crucial pour préserver l'intégrité des preuves

numériques. Nous allons détailler la création d'une image d'un disque physique, qui est l'un des scénarios les plus courants.

1. Lancement de la Création d'Image Disque

1. **Ouvrez FTK Imager** : Lancez l'application FTK Imager. Vous verrez l'interface principale.
2. **Sélectionnez 'Create Disk Image'** : Dans le menu supérieur, cliquez sur `File` (Fichier), puis sélectionnez `Create Disk Image` (Créer une image disque).

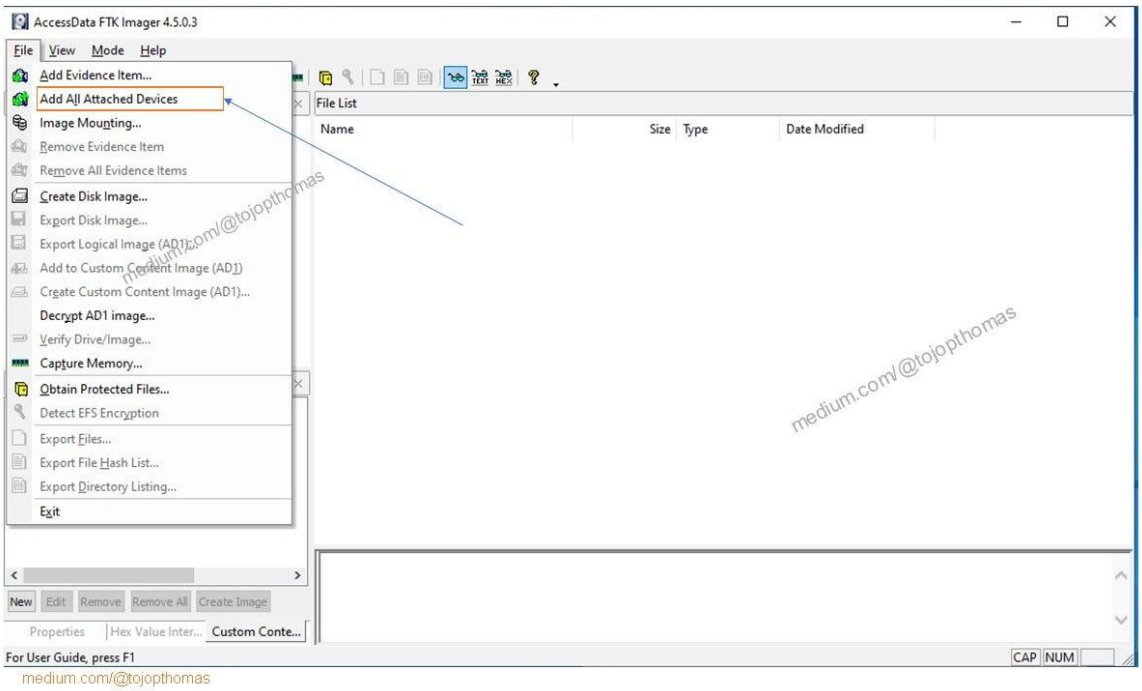

Figure 3: Accès à la fonction 'Create Disk Image' via le menu 'File'.

2. Choix du Type de Source

Une fenêtre

Montage d'une Image Disque avec FTK Imager

Une fois que vous avez créé une image forensique, il est souvent nécessaire de la "monter" pour pouvoir l'explorer comme un disque dur normal, sans altérer l'original. FTK Imager permet de monter des images en mode lecture seule, garantissant ainsi l'intégrité des preuves.

1. Lancement du Montage d'Image

1. **Ouvrez FTK Imager** : Lancez l'application FTK Imager.

2. **Sélectionnez 'Image Mounting'** : Dans le menu supérieur, cliquez sur `File` (Fichier), puis sélectionnez `Image Mounting` (Montage d'image).

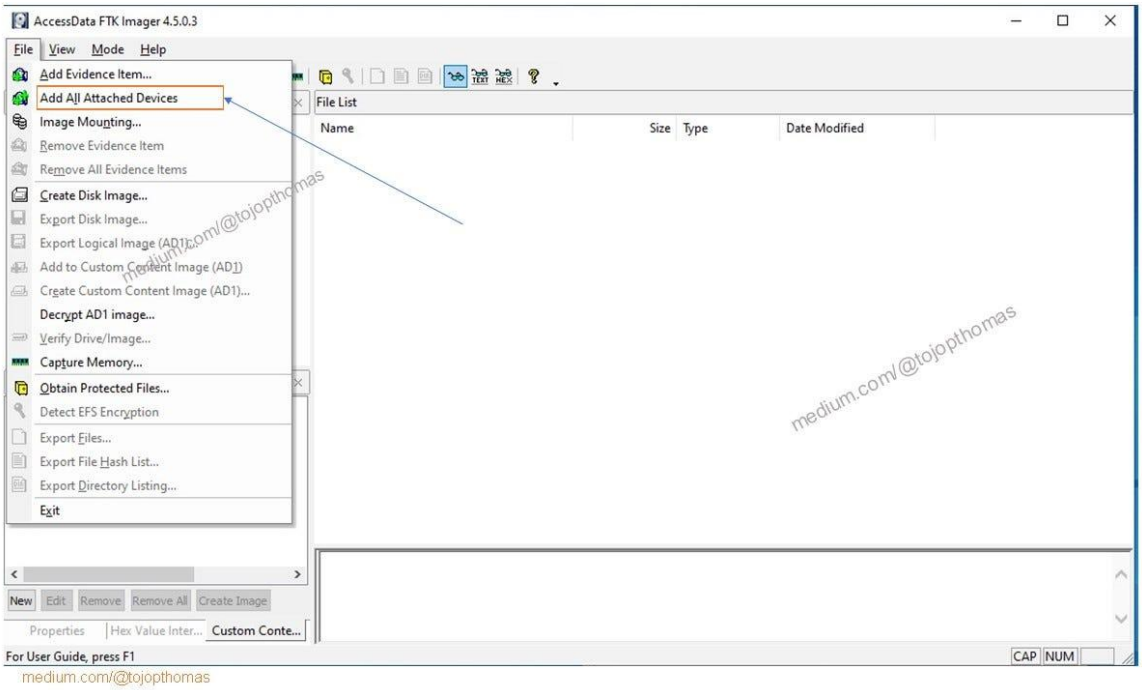

Figure 7: Accès à la fonction 'Image Mounting' via le menu 'File'.

2. Configuration du Montage

Une fenêtre 'Image Mounting' s'ouvrira, vous permettant de configurer les options de montage.

1. **Chemin de l'Image** : Cliquez sur le bouton `Add Image` (Ajouter une image) et naviguez jusqu'à l'emplacement de votre fichier d'image forensique (par exemple, un fichier `.E01`, `.DD`, ou `.AFF`). Sélectionnez le fichier et cliquez sur `Open`.

2. **Type de Montage** :

    - **Physical Drive** : Monte l'image comme un disque physique. Cela permet d'accéder à toutes les partitions et à l'espace non alloué, comme si le disque original était connecté.
    - **Logical Drive** : Monte uniquement les partitions logiques de l'image, comme des lettres de lecteur (par exemple, `D:`, `E:`). C'est utile si vous voulez simplement explorer les fichiers et dossiers visibles.

3. **Mode de Montage** :

    - **Read-Only (Recommandé)** : C'est le mode par défaut et le plus sûr. Il garantit que l'image ne sera pas modifiée pendant l'exploration, préservant ainsi l'intégrité des preuves.

- **Writable (À utiliser avec prudence)** : Permet d'écrire sur l'image montée. À n'utiliser que dans des environnements de test contrôlés et jamais avec des preuves originales, car cela altérerait l'image.

4. **Lettre de Lecteur** : Choisissez une lettre de lecteur disponible pour le montage de l'image (par exemple, `Z:`).

5. **Cliquez sur 'Mount'** : Une fois les options configurées, cliquez sur le bouton `Mount` (Monter) pour démarrer le processus de montage.

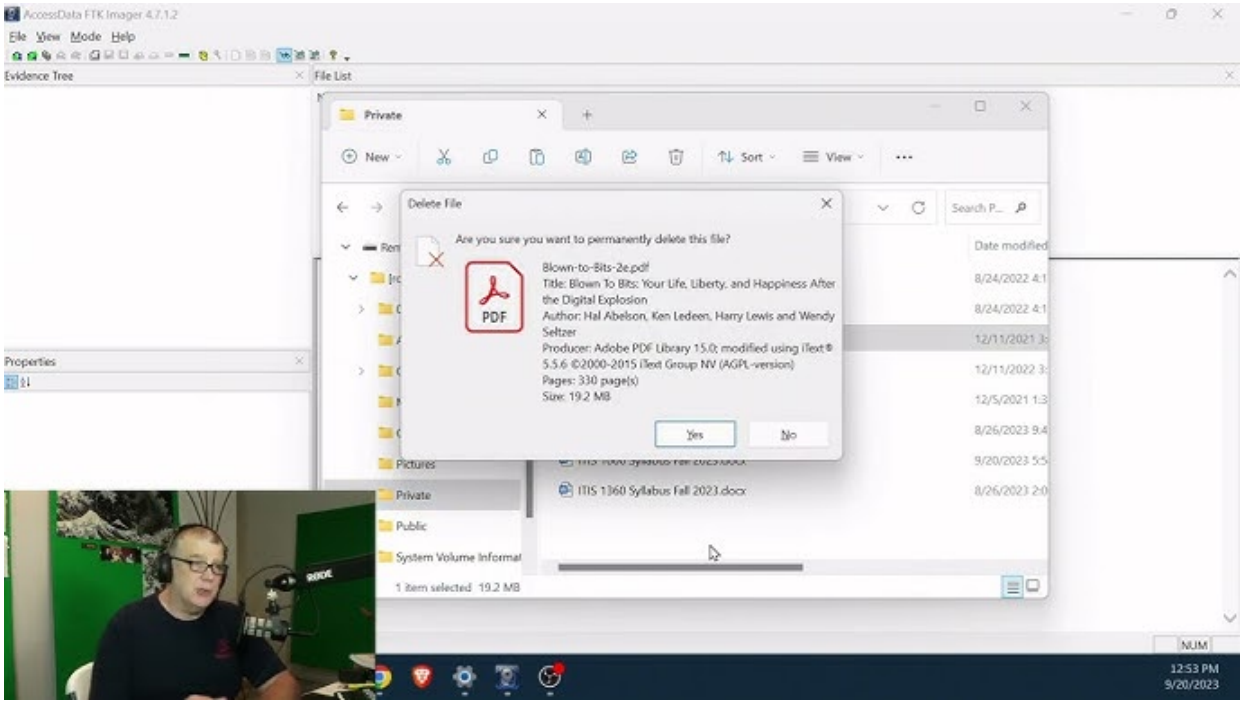

Figure 8: Configuration des options de montage d'une image disque dans FTK Imager.

3. Exploration de l'Image Montée

Une fois l'image montée avec succès, elle apparaîtra comme un nouveau lecteur dans l'Explorateur de fichiers de Windows. Vous pouvez alors l'explorer, copier des fichiers, et effectuer des analyses comme vous le feriez avec un disque dur physique, mais en toute sécurité en mode lecture seule.

```
 ![Image montée dans l'Explorateur Windows](/home/ubuntu/upload/
search_images/2kLMR9fBuERo.jpg)
*Figure 9: L'image disque montée apparaît comme un nouveau
lecteur dans l'Explorateur de fichiers de Windows.*
```

4. Démontage de l'Image

Lorsque vous avez terminé votre analyse, il est important de démonter l'image pour libérer les ressources et s'assurer qu'aucune modification accidentelle ne puisse survenir.

1. **Retournez à la fenêtre 'Image Mounting'** : Dans FTK Imager, allez dans `File` > `Image Mounting`.
2. **Sélectionnez l'Image à Démonter** : Dans la liste des images montées, sélectionnez celle que vous souhaitez démonter.
3. **Cliquez sur 'Dismount'** : Cliquez sur le bouton `Dismount` (Démonter). L'image sera alors retirée du système.

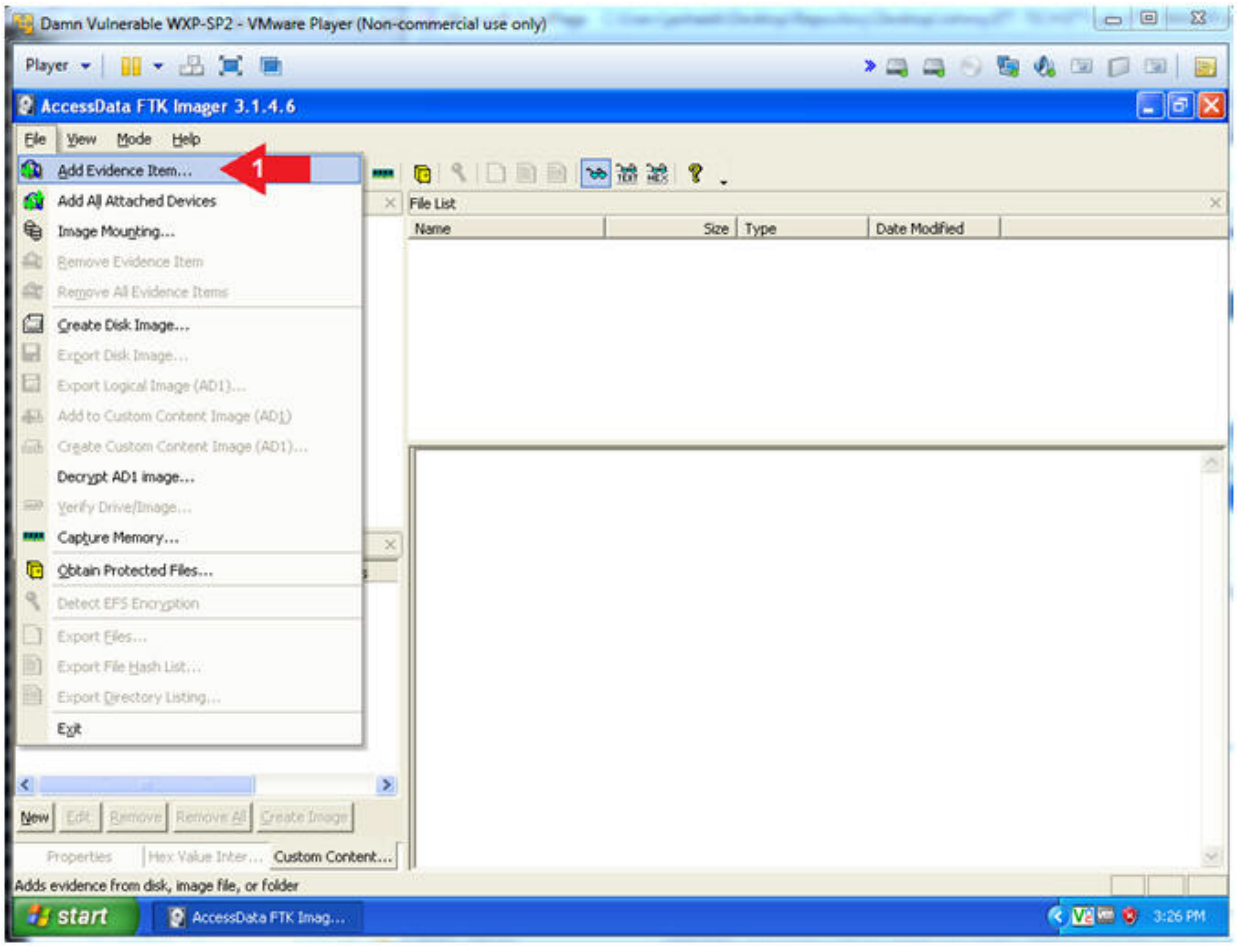

Figure 10: Démontage d'une image disque après l'analyse.

Le montage d'images est une fonctionnalité puissante de FTK Imager qui facilite l'analyse forensique en permettant une exploration non destructive des preuves numériques.

Capture de la Mémoire Vive (RAM) avec FTK Imager

La capture de la mémoire vive (RAM) est une étape essentielle en criminalistique numérique, notamment pour l'analyse des artefacts volatils (processus en cours, connexions réseau actives, clés de chiffrement, mots de passe en clair, etc.) qui disparaissent à l'extinction de l'ordinateur. FTK Imager offre une fonctionnalité simple pour réaliser cette capture.

1. Lancement de la Capture de Mémoire

1. **Ouvrez FTK Imager** : Lancez l'application FTK Imager.
2. **Sélectionnez 'Capture Memory'** : Dans le menu supérieur, cliquez sur `File` (Fichier), puis sélectionnez `Capture Memory` (Capturer la mémoire).

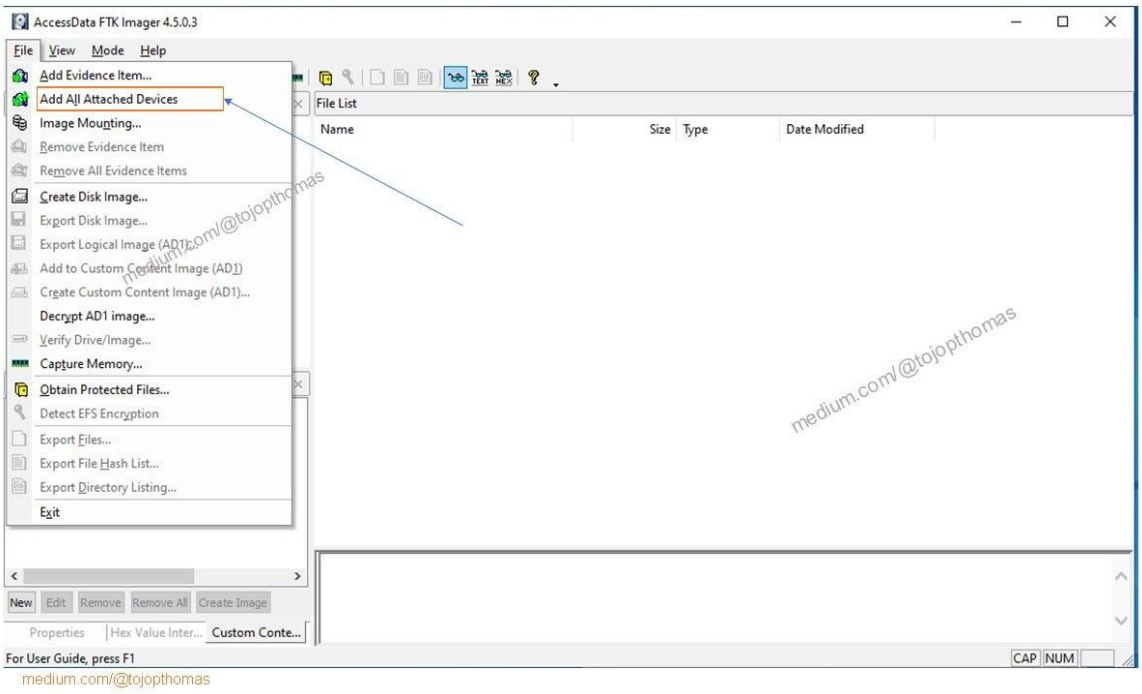

Figure 11: Accès à la fonction 'Capture Memory' via le menu 'File'.

2. Configuration de la Capture de Mémoire

Une fenêtre 'Memory Capture' s'ouvrira, vous permettant de spécifier l'emplacement et le nom du fichier de sortie.

1. **Chemin de Destination** : Cliquez sur le bouton `Browse` (Parcourir) et choisissez un emplacement pour enregistrer le fichier de vidage de la mémoire. Il est recommandé de l'enregistrer sur un support externe ou un emplacement sécurisé pour ne pas altérer le système cible.

2. **Nom du Fichier** : Donnez un nom significatif au fichier de vidage de la mémoire (par exemple, `RAM_dump_DATE_TIME.mem`). L'extension `.mem` est couramment utilisée.

3. **Inclure le Fichier d'Échange (Pagefile.sys)** : Vous avez l'option d'inclure le fichier d'échange (`pagefile.sys`) dans la capture. Le fichier d'échange est utilisé par Windows pour stocker temporairement des données de la RAM sur le disque dur lorsque la mémoire physique est pleine. L'inclure peut fournir des informations supplémentaires, mais augmentera la taille du fichier de sortie.

4. **Créer un fichier AD1 avec le fichier d'échange et les fichiers protégés** : Cette option permet de créer un fichier d'image forensique au format AD1 qui inclura le fichier d'échange et les fichiers protégés (comme le SAM, SYSTEM, SECURITY hives du registre). C'est une option très utile pour une analyse complète.

5. **Cliquez sur 'Capture Memory'** : Une fois les options configurées, cliquez sur le bouton `Capture Memory` pour démarrer le processus. La durée de la capture dépendra de la quantité de RAM et de la vitesse du disque de destination.

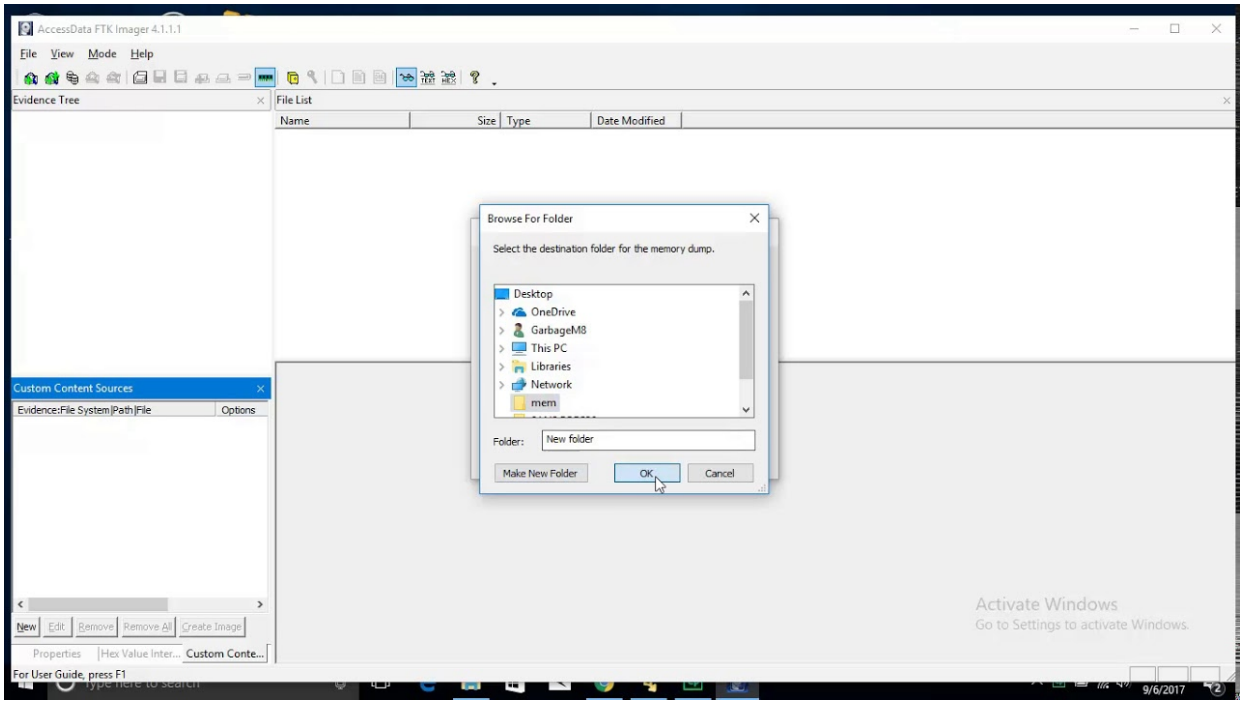

Figure 12: Configuration des options de capture de mémoire dans FTK Imager.

3. Progression et Fin de la Capture

FTK Imager affichera une barre de progression pendant la capture. Une fois terminée, un message de confirmation apparaîtra.

```
 ![Progression de la capture de mémoire](/home/ubuntu/upload/
search_images/d69i61kwrjzc.jpg)
*Figure 13: Progression de la capture de mémoire vive.*
```

Le fichier de vidage de la mémoire (`.mem` ou `.ad1`) pourra ensuite être analysé avec des outils spécialisés comme Volatility Framework pour extraire des informations précieuses.

Obtention de Fichiers Protégés avec FTK Imager

Certains fichiers sur un système d'exploitation, comme le registre Windows (SAM, SYSTEM, SECURITY) ou les fichiers de mots de passe (NTDS.dit sur les contrôleurs de domaine), sont souvent verrouillés ou protégés par le système d'exploitation en cours d'exécution. FTK Imager offre une fonctionnalité pour contourner ces protections et acquérir ces fichiers essentiels pour l'analyse forensique.

1. Lancement de l'Obtention de Fichiers Protégés

1. **Ouvrez FTK Imager** : Lancez l'application FTK Imager.
2. **Sélectionnez 'Obtain Protected Files'** : Dans le menu supérieur, cliquez sur `File` (Fichier), puis sélectionnez `Obtain Protected Files` (Obtenir les fichiers protégés).

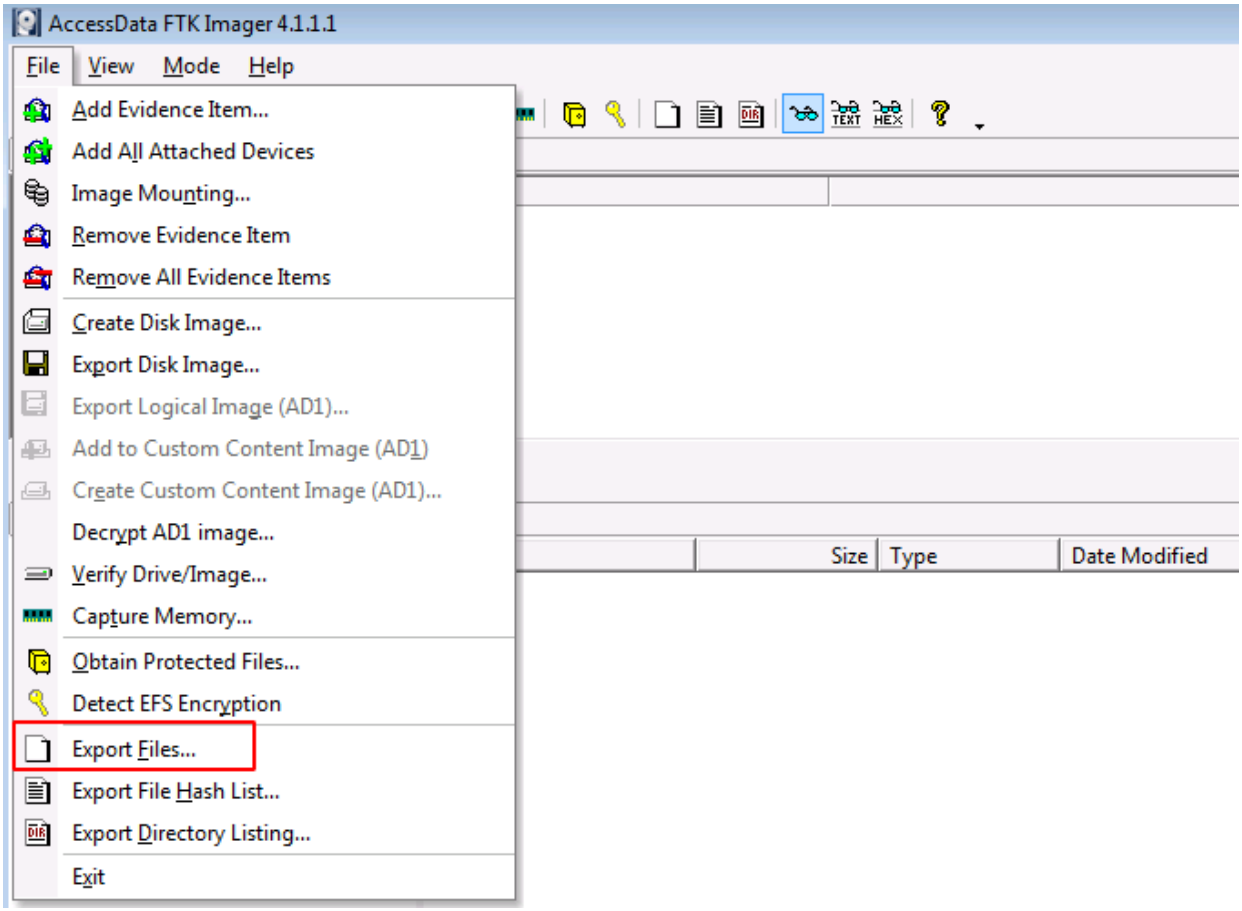

Figure 14: Accès à la fonction 'Obtain Protected Files' via le menu 'File'.

2. Configuration de l'Obtention de Fichiers Protégés

Une fenêtre 'Obtain Protected Files' s'ouvrira, vous permettant de choisir les types de fichiers à acquérir et l'emplacement de destination.

1. **Sélectionnez les Fichiers à Obtenir** : FTK Imager vous présentera une liste de fichiers protégés courants que vous pouvez acquérir. Les options typiques incluent :
    - **Password Hashes (SAM/SYSTEM/SECURITY)** : Pour extraire les hachages de mots de passe du registre Windows.
    - **NTDS.dit (Active Directory Database)** : Pour les contrôleurs de domaine, ce fichier contient les informations d'identification des utilisateurs du domaine.
    - **Other Protected Files** : D'autres fichiers système qui pourraient être verrouillés.

    Cochez les cases correspondant aux fichiers que vous souhaitez acquérir.

2. **Chemin de Destination** : Cliquez sur le bouton `Browse` (Parcourir) et choisissez un dossier de destination pour enregistrer les fichiers extraits. Il est recommandé de les enregistrer sur un support externe ou un emplacement sécurisé.

3. **Cliquez sur 'OK'** : Une fois les options configurées, cliquez sur `OK` pour démarrer le processus d'extraction.

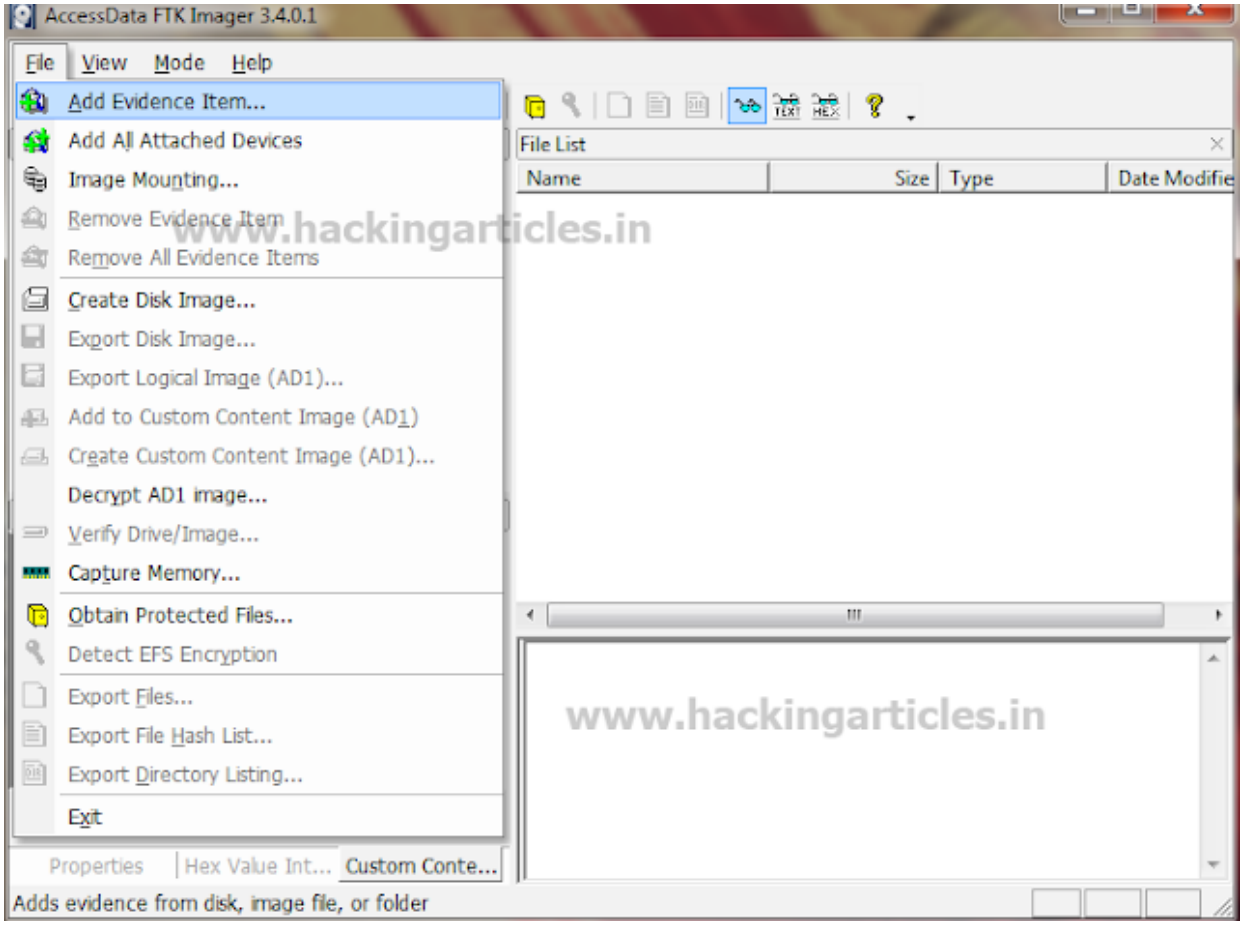

Figure 15: Configuration des options pour obtenir les fichiers protégés dans FTK Imager.

3. Progression et Fin de l'Extraction

FTK Imager affichera une barre de progression pendant l'extraction. Une fois terminée, un message de confirmation apparaîtra.

```
 ![Progression de l'extraction des fichiers protégés](/home/
ubuntu/upload/search_images/VOBCt9YPDXmg.png)
*Figure 16: Progression de l'extraction des fichiers protégés.*
```

Ces fichiers extraits sont cruciaux pour des analyses ultérieures, notamment pour le craquage de mots de passe (avec des outils comme Hashcat ou John the Ripper) ou pour l'analyse des informations d'identification du domaine.

Exportation de Fichiers et Dossiers avec FTK Imager

Après avoir acquis une image forensique ou monté une image, vous aurez souvent besoin d'exporter des fichiers ou des dossiers spécifiques pour une analyse plus

approfondie ou pour les présenter comme preuves. FTK Imager permet d'exporter des éléments individuels ou des répertoires entiers tout en préservant leurs métadonnées.

1. Navigation et Sélection des Éléments

1. **Chargez l'Image ou le Disque** : Assurez-vous que l'image forensique est chargée dans FTK Imager (soit en l'ajoutant comme élément de preuve, soit en la montant).
2. **Explorez l'Arborescence** : Dans le panneau de gauche (Evidence Tree), naviguez à travers l'arborescence du système de fichiers pour localiser les fichiers ou dossiers que vous souhaitez exporter.
3. **Sélectionnez les Éléments** : Cliquez sur les fichiers ou dossiers que vous voulez exporter. Vous pouvez sélectionner plusieurs éléments en utilisant les touches `Ctrl` ou `Shift`.

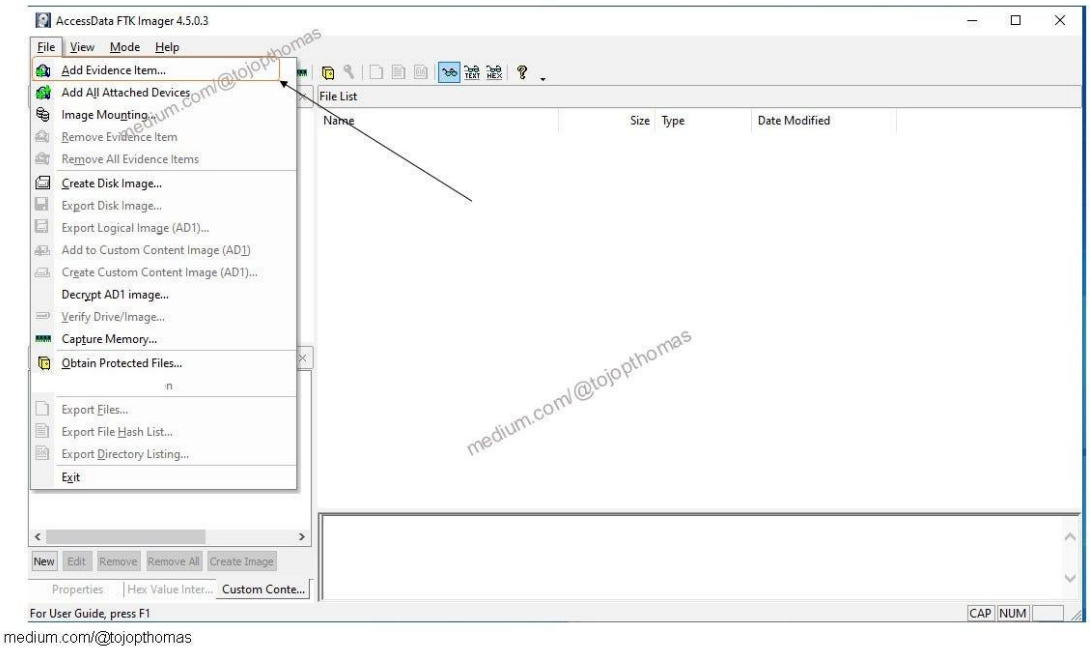

Figure 17: Navigation dans l'arborescence des preuves et sélection des fichiers à exporter.

2. Lancement de l'Exportation

1. **Cliquez Droit ou Utilisez le Menu Fichier** : Une fois les éléments sélectionnés, vous avez deux options :
    - **Clic Droit** : Cliquez avec le bouton droit de la souris sur la sélection et choisissez `Export Files` (Exporter les fichiers).
    - **Menu Fichier** : Allez dans `File` (Fichier) > `Export Files`.

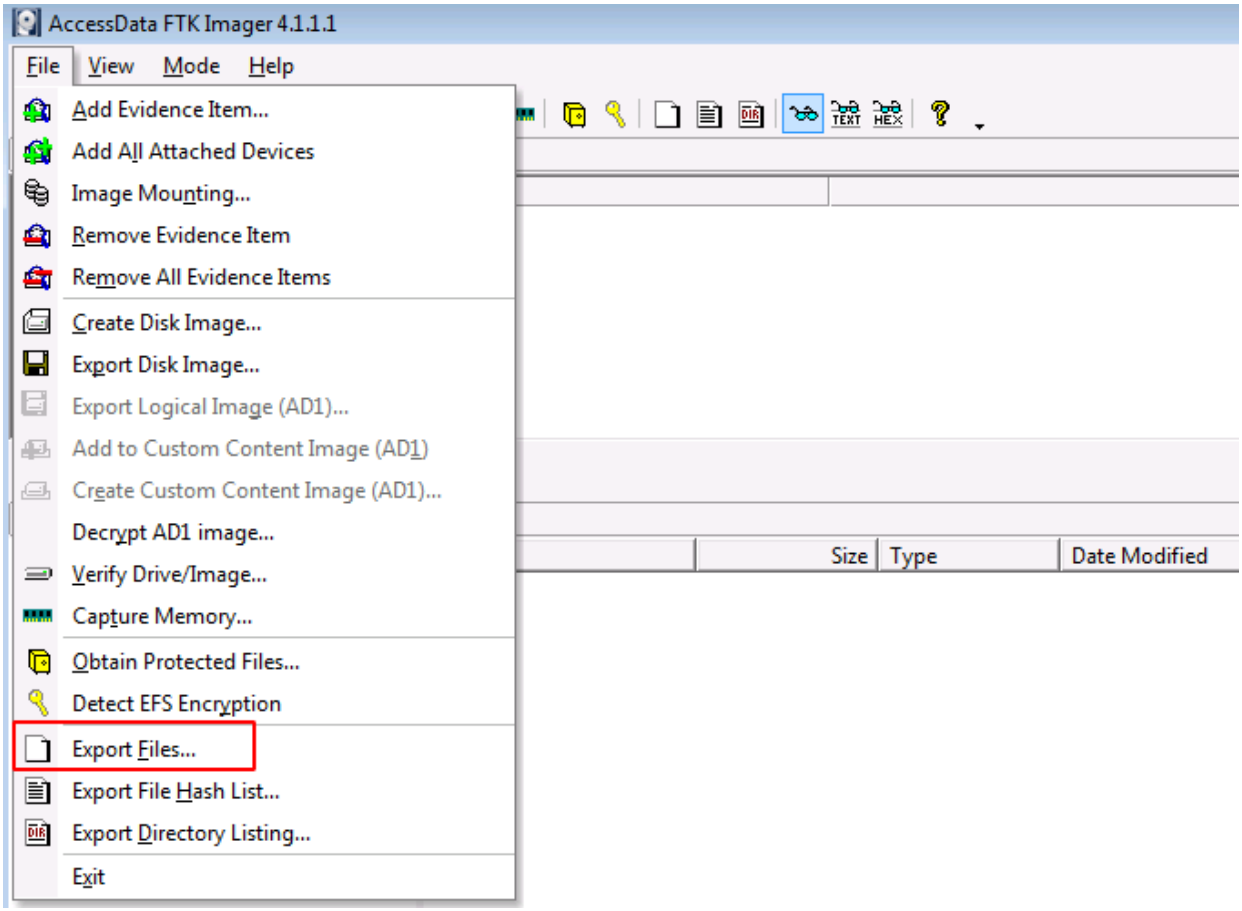

Figure 18: Accès à la fonction d'exportation de fichiers via le menu contextuel ou le menu 'File'.

3. Configuration de l'Exportation

Une fenêtre de dialogue s'ouvrira, vous demandant de spécifier l'emplacement de destination.

1. **Choisissez le Dossier de Destination** : Cliquez sur `Browse` (Parcourir) et sélectionnez le dossier où vous souhaitez enregistrer les fichiers exportés. Il est recommandé de choisir un emplacement sécurisé et organisé pour vos preuves.

2. **Cliquez sur 'OK'** : Une fois le dossier de destination choisi, cliquez sur `OK` pour lancer l'exportation.

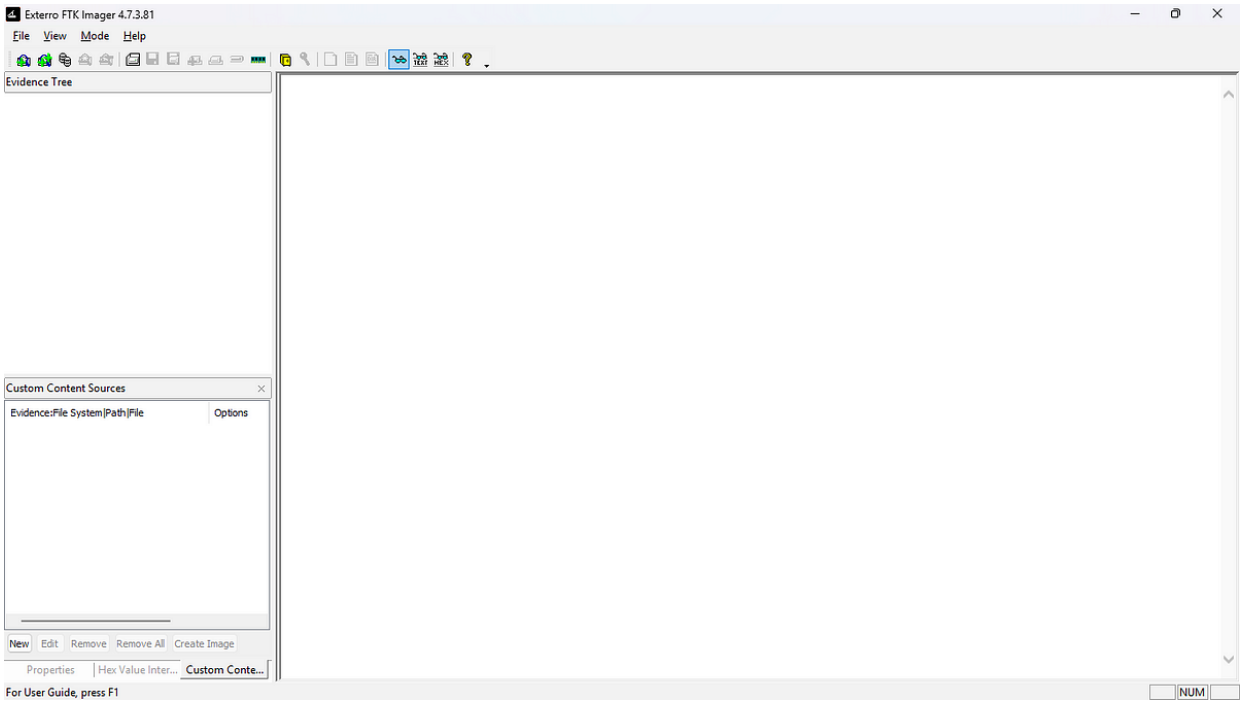

Figure 19: Sélection du dossier de destination pour les fichiers exportés.

4. Progression et Fin de l'Exportation

FTK Imager affichera une barre de progression pendant l'exportation. Une fois terminée, un message de confirmation apparaîtra.

```
 ![Progression de l'exportation des fichiers](/home/ubuntu/
upload/search_images/hX8S8ijWKRjq.png)
*Figure 20: Progression de l'exportation des fichiers et
dossiers.*
```

Les fichiers et dossiers exportés conserveront leurs noms d'origine et, dans la mesure du possible, leurs métadonnées. Cette fonctionnalité est essentielle pour isoler des éléments spécifiques d'une preuve numérique pour une analyse ciblée ou pour les partager avec d'autres outils ou parties prenantes.

Vérification d'une Image Disque avec FTK Imager

La vérification de l'intégrité d'une image forensique est une étape cruciale pour s'assurer que l'image est une copie exacte et non altérée de la source originale. FTK Imager permet de comparer les valeurs de hachage (MD5 et SHA1) de l'image avec celles calculées à partir de la source, garantissant ainsi la fidélité de la copie.

1. Lancement de la Vérification

1. **Ouvrez FTK Imager** : Lancez l'application FTK Imager.

2. **Ajoutez l'Élément de Preuve** : Si l'image n'est pas déjà chargée, allez dans `File` (Fichier) > `Add Evidence Item` (Ajouter un élément de preuve) et sélectionnez votre fichier d'image forensique.

3. **Sélectionnez l'Image à Vérifier** : Dans le panneau de gauche (Evidence Tree), sélectionnez l'image disque que vous souhaitez vérifier.

4. **Sélectionnez 'Verify Drive/Image'** : Dans le menu supérieur, cliquez sur `File` (Fichier), puis sélectionnez `Verify Drive/Image` (Vérifier le lecteur/l'image).

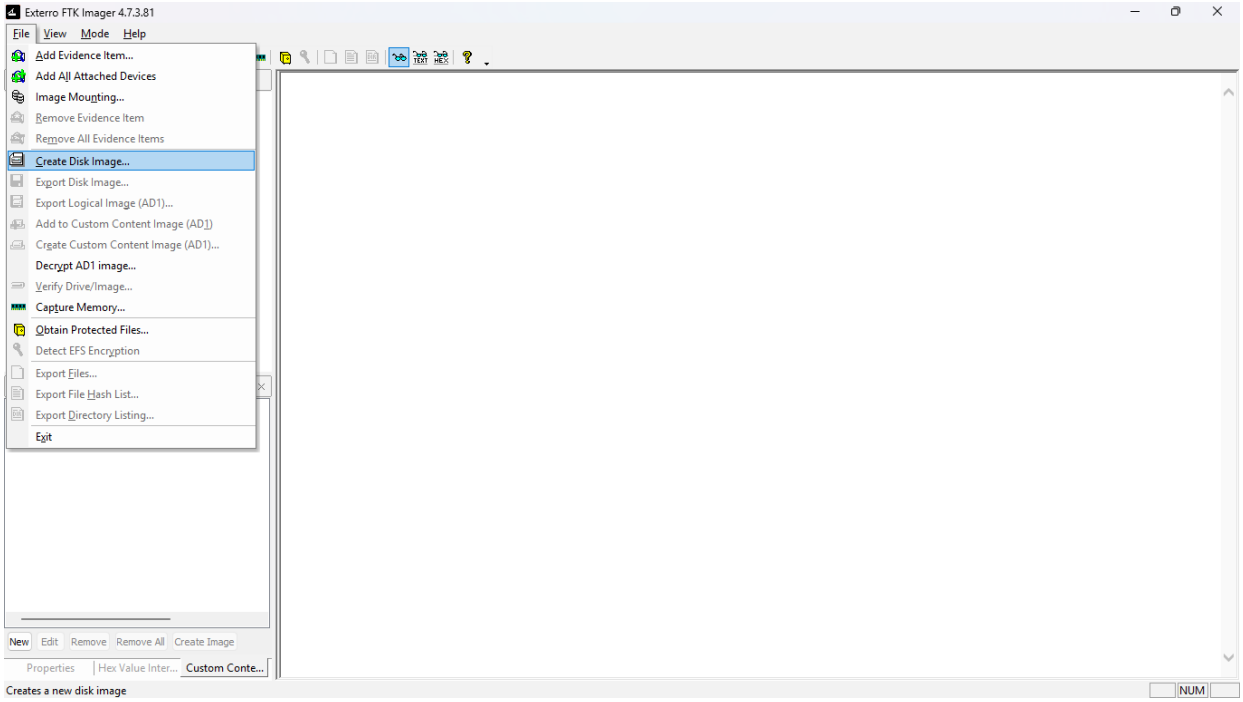

Figure 21: Accès à la fonction 'Verify Drive/Image' via le menu 'File'.

2. Processus de Vérification

FTK Imager va alors calculer les valeurs de hachage (MD5 et SHA1) de l'image et les comparer avec les valeurs de hachage qui ont été enregistrées lors de la création de l'image (si elles ont été incluses).

```
 ![Progression de la vérification de l'image](/home/ubuntu/
upload/search_images/ciTJIOykiXzC.png)
*Figure 22: Progression de la vérification de l'intégrité de
l'image disque.*
```

3. Résultats de la Vérification

Une fois le processus terminé, une fenêtre 'Drive/Image Verify Results' s'affichera, présentant les résultats de la comparaison des hachages.

- **MD5 Hash** : Affiche le hachage MD5 calculé et le compare avec le hachage stocké. Le statut doit être `Match` (Correspondance).
- **SHA1 Hash** : Affiche le hachage SHA1 calculé et le compare avec le hachage stocké. Le statut doit également être `Match`.

- **Bad Blocks List** : Indique si des blocs défectueux ont été trouvés dans l'image. Idéalement, cette liste devrait être vide.

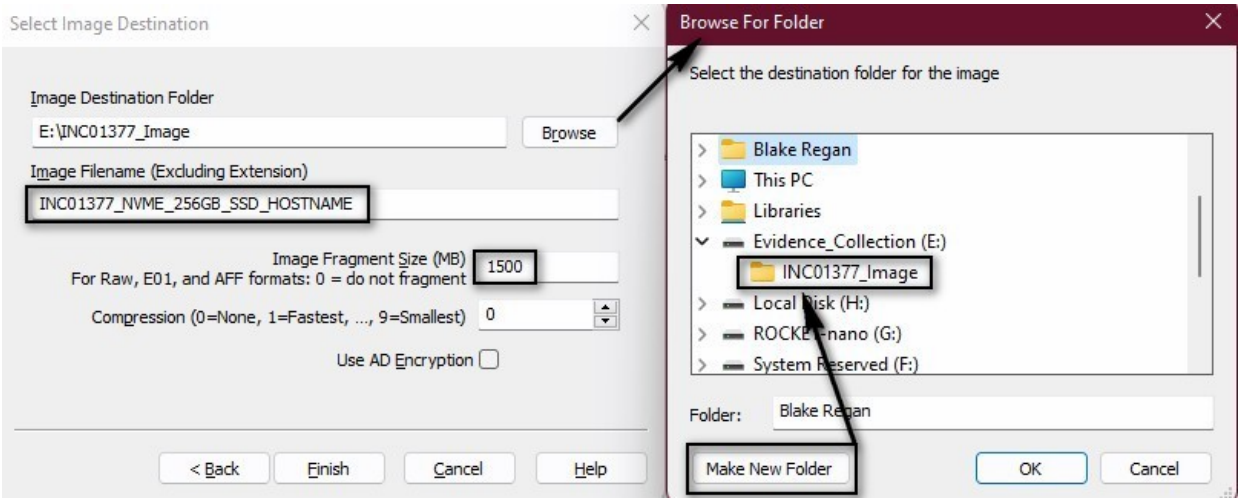

Figure 23: Résultats de la vérification de l'image, confirmant l'intégrité des données.

Si les hachages correspondent et qu'aucun bloc défectueux n'est signalé, cela confirme que l'image forensique est une copie bit-à-bit exacte de la source originale et que son intégrité a été préservée. Cette étape est fondamentale pour la recevabilité des preuves numériques en justice.

Conclusion : FTK Imager, Votre Allié en Criminalistique Numérique

FTK Imager est bien plus qu'un simple outil de copie de données ; c'est une pierre angulaire de la criminalistique numérique. Sa capacité à créer des images forensiques bit-à-bit, à monter ces images en toute sécurité, à capturer la mémoire vive et à extraire des fichiers protégés en fait un utilitaire indispensable pour tout professionnel de la sécurité ou de l'investigation.

En maîtrisant FTK Imager, vous vous assurez que vos acquisitions de preuves numériques sont réalisées avec la plus grande intégrité, garantissant leur recevabilité et

leur fiabilité dans le cadre d'une enquête ou d'une procédure judiciaire. C'est un outil qui, par sa simplicité d'utilisation et sa robustesse, permet de se concentrer sur l'analyse des données plutôt que sur les défis techniques de l'acquisition.

Nous espérons que ce manuel détaillé vous aura fourni les connaissances nécessaires pour utiliser FTK Imager de manière efficace et professionnelle. N'oubliez jamais l'importance de la chaîne de conservation des preuves et de l'intégrité des données dans toutes vos opérations forensiques.