TD IFO3 2021

PREALABLE

Vous êtes expert judiciaire et vous avez été commissionné par un Juge d'Instruction en vue de réaliser une expertise judiciaire. L'affaire concerne des faits de faux et d'usage de faux en écriture publique, par la réalisation de faux diplômes scolaires.

L'image d'un disque dur de l'ordinateur, utilisé par la personne mise en examen, a été réalisée par un enquêteur spécialisé et elle vous a été remise en même temps que la commission d'expertise.

Cette image est composée d'un fichier unique au format numérique « e01 ».

La mission pour laquelle vous est commissionnée est la suivante :

« « ***Bien vouloir procéder à l'expertise de l'image du disque dur, en vue de rechercher toutes les traces et tous les éléments pouvant avoir un rapport avec des faits de confection, modification de diplômes universitaires. Le mis en examen déclare n'avoir rien à se reprocher, il pourrait toutefois avoir des complices.***

A l'issue de vos investigations, bien vouloir nous remettre un rapport détaillé mentionnant les éléments ayant un lien avec les faits dénoncés démontrant ou non l'implication du mis en examen » ».

Conseils :

Le principal logiciel utilisé sera : Autopsy. Il pourra être complété par différents outils pré-installés sur les machines virtuelles ou téléchargés lors du TD.

COMPREHENSION DE L'UTILITE D'AUTOPSY

Monter l'image du disque dur dans l'explorateur Windows afin de comparer les dossiers visibles dans l'explorateur et ceux visibles dans Autopsy. (OSF MOUNT)

- Quels sont les différences notables ?
- Pouvez-vous accéder à tous fichiers dans l'explorateur Windows ?
- Qu'en concluez-vous ?

INSTALLATION ET CONFIGURATION DU SYSTEME

- Combien y a-t-il de partitions ? Et quels sont leurs types ?
- De quel système d'exploitation s'agit-il ?
- Quand a-t-il été installé ?
- Quel est l'utilisateur déclaré lors de cette installation ? Y-a-il d'autres utilisateurs ?
- Quels sont les périphériques qui ont été connectés à la machine ?

UTILISATEURS

- Identifier les utilisateurs et lister leurs dossiers personnels
- Quel est le dernier utilisateur de la machine ?
- Quels sont les derniers documents et fichiers auxquels il a accédé ?

IDENTIFICATION DES NAVIGATEURS

- Lister tous les navigateurs configurés sur le support.
- Extraire les historiques de navigations de ces navigateurs.
- Mettez en évidence les éléments de recherches pouvant avoir un lien avec des faux diplômes.

AFFICHAGE DES DOCUMENTS

- Lister tous les documents word, excel et txt présents sur le support. (Vous pouvez exclure les fichiers présents dans le dossier « \windows » et « \OEM »
- Avez-vous trouvé le fichier « tarif-diplômes.xlsx » ? Que pouvez-vous dire sur ce fichier ? Quelle est son origine ?
- Lister tous les documents PDF présents. Vous pouvez exclure tous les fichiers présents dans « \Program files » et « «\OEM ».
- Quels sont les auteurs de tous ces fichiers ?

AFFICHAGE DES IMAGES

- Lister tous les dossiers de l'utilisateur « UTT3MSFOR » contenant des fichiers de type image.
- Extraire toutes les images se trouvant dans les dossiers personnels de l'utilisateur (hors Appdata, Program files etc…)
- Afficher l'image dont le hash est « 5F089B7F8F1D4BBA632A37BF58FBEDB7» (MD5) et l'image dont le hash est « 0E3F307638737FB23838CB6B2C99A4AE308110B8 » (SHA-1).
- Ces images sont-elles stockées dans plusieurs dossiers, si oui lesquelles ?
- Afficher l'image dont le hash MD5 est « D20B3D300F78D9CF417F76400FD1BD90 ». Qu'en pensez-vous ? Avez-vous trouvé d'autres images de même type ?

METADONNEES

- Extraire toutes les métadonnées des images présentes dans les dossiers de l'utilisateur « UTT3MSFOR ».
- Distinguer les images contenant des données de géolocalisation.

CLOUD

- Avez-vous identifié différents services de cloud computing ?
- Contiennent-ils des fichiers ou des dossiers ?

FICHIERS CHIFFRES

- Rechercher et afficher le fichier dont le hash est« EBBEE4596DA1AA3868FC0B07A24CA894CF95DF14» (Sha-1). Arrivez vous à ouvrir ce fichier ?
- Si vous ne l'avez pas remarqué auparavant, effectuer une recherche du fichier « mdp.txt », il vous permettra peut-être d'y arriver. Que contient ce fichier ?
- Rechercher et afficher le fichier dont le hash est « FC31AEC191149029B86E315B0C76B90D6EFDC97F» (sha-1). Arrivez vous à ouvrir ce fichier ?

MESSAGERIE

- Lister les applications de messagerie installées ?
- Pouvez vous extraire les messages qu'elles contiennent ? Dans les emails avez-vous trouver des éléments avec l'affaire en cours ?
- Extraire les données techniques d'un email afin d'obtenir les adresses emails utilisées et les adresses IP.

DIVERS

- Avez-vous trouvé un backup de téléphone ?
- Lister tout ce que vous avez trouvé et qui ne figure pas dans les différentes questions précédentes.
- Sur cette machine, les applications Facebook, Facebook Messenger, skype et Courrier ont été utilisées via les tuiles. Des traces sont sans doute présentes, arrivez vous à les mettre en évidence ? (user\appdata\local\package\....) (laisser tomber si vous butez dessus, passez à la conclusion).

CONCLUSION

Tirer les conclusions de tous les éléments que vous avez mis en évidence. Pouvez vous conclure qu'il y a des éléments permettant de penser qu'il y a des faux documents sur ce supports créés par des utilisateurs ?