Étude de cas – Posinc

Formulaire de réponse

Votre nom (Polytechnique) : Amadou Moctar Ndiaye 2168458 (équipe K)

Votre numéro d'équipe (Laval) :

Média trouvé?	Clé USB 256Go
Contient des preuves?	Oui
Options OCICE	OCICE
Décision imposée	Saisir un clone forensique

22.5/23

Options à exclure : donner justifications suffisantes Maximum **{3 pts}** 2.5/3	**Éliminer << Original >> :** • La clé USB de 256Go appartient à Jean Saies • Il y'a présence d'effet personnel tels que des vidéos et photos de Jean Saies et de son fils lors d'évènements important comme sa graduation, une compétition de nation ou il gagne la médaille d'or etc… Incomplet: saisir l'original serait une intrusion (Matériel et Durée) déraisonnable compte tenu de la disponibilité d'autres modes et du type de fichiers contenant la preuve. **Éliminer << Copie ciblée >> :** • Pas le temps de faire un examen complet de clé **car** pour bidouiller les bases de données contenues dans la clé de manière à contoumer les restrictions du logiciel, avec l'aide du fabriquant, il nous faudrait une journée entière **or** on a une limite de temps pour la perquisition. • Il y'a un risque à l'intégralité car certains fichiers se trouvent dans un répertoire dont l'accès est interdit même à l'administrateur de la compagnie. • Beaucoup de données sur la clé (des centaines de fichiers protégés) or le temps nous est limité **Éliminer << Copie forensique extensive >> :** • La preuve qu'on a repérée est un vestige de donnée et ce n'est pas facile à copier de façon forensique.

Faits et circonstances Maximum **{10 pts}** 10 / 10	**<u>Nature du média :</u>** Le média est une clé USB de 256Go, **<u>donc</u>** accessible avec mon ordinateur de fouille et les ordinateurs du laboratoire. **<u>Utilisation réelle présente et passé du média :</u>** Le média est utilisé en tant que média d'archivage et opérationnel **<u>Puisque</u>** nous y trouvons une base de données contenant des transactions datant d'il y'a 10ans, des fichiers datant d'il y'a 2ans et d'autres plus récents datant seulement d'hier **<u>donc</u>** de la période sous investigation. **<u>Taille du média :</u>** Le média a une taille de 256Go **<u>donc</u>** son contenu peut être facilement sauvegardé sur un même média qu'on peut facilement trouver à un prix dérisoire dans un magasin électronique **<u>Nature des données :</u>** Données accessibles avec le logiciel d'origine car les données sont stockées dans des centaines de fichiers se trouvant sur la clé USB avec comme extension .pbz, ce qui est compliqué à extraire car il faudra utiliser le logiciel PlusssBizard **<u>Valeurs probantes des données :</u>** La valeur probante du contenu des données est élevée **<u>car</u>** le répertoire C:\Users\JeanSaies\Documents contient des documents dont le contenu correspond à ce qui est recherché dans le cadre de la perquisition donc ce qui prouve que Jean Saies ou son entourage ont eu accès à des informations confidentielles. **<u>Perte éventuelle d'informations et volatilité des données :</u>** le fabricant précise qu'il n'en met pas à la disposition des autorités que le fait d'avoir une copie du logiciel ne nous donne pas forcément accès aux données. **<u>Limitation à l'accès :</u>** : La clé USB possède un port USB courant sur la plupart des ordinateurs. L'accès au contenu ne constitue donc pas un obstacle ni pour l'image ni pour le clone.

	<u>Limitations inhérentes au média cible</u> : Les médias de même type et même interface que la clé USB de Jean Saies sont faciles à obtenir chez n'importe quel magasin électronique et à prix modique. Ceci ne constitue **<u>donc</u>** pas un obstacle pour l'image ni pour le clone. **<u>Usage projeté de l'artéfact :</u>** Nous prévoyons une analyse approfondie du média afin de trouver d'autres vestiges de données qui, une fois associées aux documents se trouvant dans le répertoire C:\Users\JeanSaies\Documents, permettrait de cerner le suspect.

Impacts de choisir chaque option Maximum **{10 pts}** 10/10	**<u>Intégralités de la preuve :</u>** On un niveau confortable de certitude qu'on sera en possession de toutes les preuves pertinentes car Cloner ou imager le média (clé USB 256Go) nous permet de préserver l'intégrité des preuves. **<u>Règle de la meilleure preuve :</u>** La meilleure preuve est l'original **<u>cependant</u>** en clonant ou en imageant le média on est en mesure d'avoir la même valeur probante que 'original **<u>car</u>** ça nous permet de copier à la fois les éléments irréels et réels. Alors la preuve ne perd donc pas en qualité. Excellente remarque Bravo!! **<u>Force :</u>** n'est pas minimale puisqu'on empêche Jean Saies de profiter de son bien. Il y'a utilisation de la <u>force immanente</u> **<u>car</u>** Jean Saies est dans un endroit rempli d'investigateurs et toute l'attention se centre sur lui. Il y'a aussi l'utilisation de la <u>force par privation de jouissance</u> **car** Jean Saies se voit son espace personnel, qu'il s'est psychologiquement approprié, envahi par les investigateurs. Il y'a aussi utilisation de la force psychologique dans le sens ou Jean Saies, ne sachant pas si nous arriverons à extraire toutes les données du média trouvé et surtout savoir le contenu de tous les fichiers. pbz, sera craintif d'éventuelles poursuites contre lui. **<u>Interruption minimale des opérations d'entreprises ou des fonction domestiques :</u>** Il y'a interruption des opérations d'entreprises pour un bon bout de temps d'autant plus que Jean Saies est présent au bureau lors de notre perquisition. **<u>Intrusion :</u>** L'intrusion n'est pas minimale **car** Jean Saies est présent dans le lieu de perquisition donc il subit : ○ La durée de notre présence pendant tout le long de la perquisition (de 09h10 du matin à 20H30 du soir) ○ L'ampleur de l'utilisation de son équipement. Il y'a privation de jouissance du matériel, car ce dernier est saisi. ○ L'ampleur de l'utilisation de notre propre équipement.

	<u>Vie privée :</u> Il y'a intrusion dans tout son aspect privé en analysant le média. Mais l'intrusion est minimale compte tenu des bornes de vie privée suivantes : ○ **Hygiène générale :** En installant son bureau de travail dans son appartement et en y laissant son clé USB, jean Saies renonce en partie à son droit à la vie privée. ○ **Relation avec l'activité reprochée :** Les documents trouvés dans le répertoire C:\Users\JeanSaies\Documents, dont le contenu correspond à ce qui recherché dans le cadre de la perquisition, constituent une preuve importante qu'il a été en possession, volontairement ou pas, de preuves se rapportant au crime en question. ○ **Droit objectif au secret :** Il reste néanmoins des expectatives résiduelles de vie privée tels que les photos de famille de Jean Saies. ○ **Mesure de protection et de contrôle :** Mesure mise en place pour protéger les données du média car des mots de passe et un logiciel de déchiffrage sont associés à quasiment tous les fichiers de la clé USB. ○ **Niveau de diffusion :** L'information considérée est placée dans un lieu inaccessible à tous d'où l'existence de mots de passe pour protéger les fichiers du média. **<u>Discrétion :</u>** La discrétion sera assurée à l'égard des éléments trouvés sur la clé USB de Jean Saies.
Décision	Saisir un clone forensique