**Formulaire de réponse**

**Étude de cas Posinc**

**Vos nom et prénom : Tran Simon**

**Votre numéro matricule : 1961278**

Cette section doit **obligatoirement** constituer la page 1 de votre rapport

Veuillez **mettre en surbrillance** la mission qui vous a été assignée

|  |  |  |  |
| --- | --- | --- | --- |
| Média trouvé? | Ordinateur portatif corporatif | Clé USB 256 Go | Ordinateur portatif personnel |
| Contient des preuves? | Oui | Oui | Oui |
| Options OCICE | OCICE | OCICE | OCICE |
| Décision imposée | Saisir l’original | Saisir un clone forensique | Saisir une image forensique |

|  |  |  |  |
| --- | --- | --- | --- |
| Média trouvé? | Cellulaire corporatif Samsung | Disque externe My Passport Wireless Pro | Microsoft Surface Pro 7 Twister |
| Contient des preuves? | Oui | Oui | Oui |
| Options OCICE | OCICE | OCICE | OCICE |
| Décision imposée | Saisir l’original | Saisir une copie forensique ciblée | Saisir une image forensique |

À justifier : Veuillez consulter l’assignation qui vous a été ou vous sera transmis

Les options à exclure doivent être en **page 2** de votre rapport et tenir sur **1 seule page**

Les faits et circonstances doivent **obligatoirement** constituer les **pages 3 et 4**

L’analyse des impacts doit **obligatoirement** constituer les **pages 5 et suivantes** (sans limite de quantité)

Le rapport doit **obligatoirement être imprimé en pdf** avant d’être remis.

|  |  |
| --- | --- |
| Décision | Inscrire le média assigné et la décision qui s’y rattache  **Cellulaire Corporatif Samsung : Saisir l’original** |
| Options à exclure : donner justifications suffisantes  Maximum  **{10 pts}** | **Exclure Imager**   * Créer une image prendrait du temps, **or** la perquisition est limitée dans le temps * Imager risque de modifier des données, **or** on veut avoir accès à toutes les données telles qu’elles étaient au moment de la perquisition * Imager ne copie pas les bits provenant de l’espace libre du disque dur. Ainsi, les fichiers supprimés ne sont pas copiés. **Or**, puisque le téléphone provient de la compagnie et a manifestement été utilisé pour les actes criminels, on veut être certain d’avoir les fichiers supprimés, puisqu’ils pourraient contenir des preuves.   **Exclure Copier de façon ciblée**   * Il y a une centaine de fichiers audio et écouter chaque fichier prendrait trop de temps. **Or**, la perquisition est limitée dans le temps, il est **alors** impossible de copier que les fichiers qui contiennent des preuves.   **Exclure Copier de façon extensive**   * Le média est un téléphone cellulaire, il n’est **donc** pas évident de copier de façon forensique, **puisque** ce n’est pas qu’un simple disque dur. |

|  |  |
| --- | --- |
| Faits et circonstances  Maximum  **{35 pts}** | **Nature du média :** Le média est un téléphone cellulaire Samsung Galaxy 8 avec le système d’exploitation Android #XYZ Drumstick. L’appareil n’est pas sécurisé (pas de NIP ou mot de passe…), **alors** on peut librement le démarrer et parcourir les données ou même le brancher à un ordinateur et utiliser un logiciel tel que CellSpy Pro pour parcourir son contenu.  **Utilisation réelle présente et passée du média :** Le cellulaire est utilisé de façon courante, **puisqu’un** appel a été effectué il y a peu de temps (11 mars 20XX à 17h33). **Puisque** nous sommes en avril et que l’enquête a débuté il y a trois mois, l’appel a été effectué durant la période sous investigation.  **Taille du média :** Selon GSM Arena, le Samsung Galaxy A8 peut être configuré avec 32 Go ou 64 Go de stockage en plus d’une carte microSDXC[[1]](#footnote-1). La taille du média est **donc** soit de 32 Go ou 64 Go et le contenu peut **donc** être sauvegardé sur un périphérique de stockage externe qu’on peut acheter dans un magasin d’électronique. Si le téléphone est équipé d’une carte microSDXC, cette dernière pourrait être d’une taille de 32 Go jusqu’à 2 To[[2]](#footnote-2). **Ainsi,** il est possible de copier son contenu sur un disque dur externe, **puisqu’il** existe aujourd’hui des disques durs externes ayant une capacité plus grande pour un prix raisonnable.  **Nature des données :** Le téléphone contient des fichiers audios et des images. Ces fichiers sont **donc** facilement lisibles avec des logiciels communs.  **Valeur probante des données :** La valeur probante du contenu des fichiers audios est élevée, **car** un appel a été fait avec un camion pendant la période d’investigation et on discute de la diète. **Ainsi**, cela laisse croire que Jean Saies a demandé au camion d’aller chercher de la contrebande.  **Perte éventuelle d’information :** Le cellulaire a été retrouvé dans un état endommagé (vitre de l’écran brisée en partie), **alors** il est possible que des composants internes aient été endommagés. De plus, un écran endommagé réduit la résistance à l’eau d’un appareil. Il y a **donc** un risque que des données soient perdues si l’état de l’appareil se détériore ou si Jean Saies continue de l’utiliser et l’endommage par accident.  **Limitation à l’accès :** L’appareil n’est pas sécurisé par un NIP ou un mot de passe, il n’y a **donc** pas d’obstacle à lire ou copier les données. |

|  |  |
| --- | --- |
| Impacts de choisir chaque option  Maximum  **{45 pts}** | Il n’y a pas de limite au nombre de pages que peuvent comporter votre réponse pour la présente section. |

Professionnalisme (incluant la qualité du français) et respect des directives : 10 points

Pour les gens dont la langue maternelle n’est pas le français, on demande un effort de bonne écriture.

Références :

<https://www.gsmarena.com/samsung_galaxy_a8_(2018)-8886.php>

<https://www.kingston.com/en/blog/personal-storage/microsd-sd-memory-card-guide>

1. <https://www.gsmarena.com/samsung_galaxy_a8_(2018)-8886.php> [↑](#footnote-ref-1)
2. <https://www.kingston.com/en/blog/personal-storage/microsd-sd-memory-card-guide> [↑](#footnote-ref-2)