

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 portable corporatif	Clé USB 256 Go	Ordinateur portable 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 <b>Cellulaire Corporatif Samsung : Saisir l'original</b>
Options à exclure : donner justifications suffisantes  Maximum <b>{10 pts}</b>	<p><b>Exclure Imager</b></p> <ul style="list-style-type: none"> <li>• Créer une image prendrait du temps, <b>or</b> la perquisition est limitée dans le temps</li> <li>• Imager risque de modifier des données, <b>or</b> on veut avoir accès à toutes les données telles qu'elles étaient au moment de la perquisition</li> <li>• Imager ne copie pas les bits provenant de l'espace libre du disque dur. Ainsi, les fichiers supprimés ne sont pas copiés. <b>Or</b>, 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.</li> </ul> <p><b>Exclure Copier de façon ciblée</b></p> <ul style="list-style-type: none"> <li>• Il y a une centaine de fichiers audio et écouter chaque fichier prendrait trop de temps. <b>Or</b>, la perquisition est limitée dans le temps, il est <b>alors</b> impossible de copier que les fichiers qui contiennent des preuves.</li> </ul> <p><b>Exclure Copier de façon extensive</b></p> <ul style="list-style-type: none"> <li>• Le média est un téléphone cellulaire, il n'est <b>donc</b> pas évident de copier de façon forensique, <b>puisque</b> ce n'est pas qu'un simple disque dur.</li> </ul>

<p>Faits et circonstances</p> <p>Maximum {35 pts}</p>	<h2><u>Relatifs au média</u></h2> <p><b>Nature du média :</b></p> <ul style="list-style-type: none"> <li>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...), <b>alors</b> 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.</li> <li>L'écran du cellulaire est fracassé. Il possible (mais peu probable) que cela a été causé par l'accident de camion ou que ce soit simplement une <b>coïncidence</b>.</li> </ul> <p><b>Utilisation réelle présente et passée du média :</b> Le cellulaire est utilisé de façon courante, <b>puisque</b> un appel a été effectué il y a peu de temps (11 mars 20XX à 17h33). <b>Puisque</b> 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.</p> <p><b>Taille du média :</b> Selon GSM Arena, le Samsung Galaxy A8 peut être configuré avec 32 Go ou 64 Go de stockage en plus d'une carte microSDXC<sup>1</sup>. La taille du média est <b>donc</b> soit de 32 Go ou 64 Go et le contenu peut <b>donc</b> 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<sup>2</sup>. <b>Ainsi</b>, il est possible de copier son contenu sur un disque dur externe, <b>puisque</b> il existe aujourd'hui des disques durs externes ayant une capacité plus grande pour un prix raisonnable.</p> <h2><u>Relatifs aux données</u></h2> <p><b>Nature des données :</b> Le téléphone contient des fichiers audios et des images. Ces fichiers sont <b>donc</b> facilement lisibles avec des logiciels communs.</p> <p><b>Valeur probante des données :</b> La valeur probante du contenu des fichiers audios est élevée, <b>car</b> un appel a été fait avec un camion pendant la période d'investigation et on discute de la diète. <b>Ainsi</b>, cela laisse croire que Jean Saies a demandé au camion d'aller chercher de la contrebande.</p> <p><b>Perte éventuelle d'information :</b> Le cellulaire a été retrouvé dans un état endommagé (vitre de l'écran brisée en partie), <b>alors</b> 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 <b>donc</b> 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.</p> <h2><u>Relatifs aux limitations techniques ou aux limitations à l'accès :</u></h2> <p><b>Limitation à l'accès :</b> L'appareil n'est pas sécurisé par un NIP ou un mot de passe, il n'y a <b>donc</b> pas d'obstacle à lire ou copier les données. On peut brancher le cellulaire à un ordinateur et parcourir ses fichiers comme si c'était un disque dur externe.</p>
---	--

<sup>1</sup> [https://www.gsmarena.com/samsung\\_galaxy\\_a8\\_\(2018\)-8886.php](https://www.gsmarena.com/samsung_galaxy_a8_(2018)-8886.php)

<sup>2</sup> <https://www.kingston.com/en/blog/personal-storage/microsd-sd-memory-card-guide>

## **Divers**

**Usage projeté de l'artéfact :** Nous prévoyons écouter les fichiers audios **afin de** déterminer s'ils contiennent des preuves. De plus, nous allons chercher s'il y a d'autres fichiers compromettants ou s'il y a des informations sur l'historique de la localisation du cellulaire, **puisque** cela nous permettrait de savoir si le cellulaire se trouvait sur les lieux de l'accident.

<p>Impacts de choisir chaque option</p> <p>Maximum {45 pts}</p>	<p><b><u>Intégralité de la preuve :</u></b></p> <p>On a un niveau confortable de certitude que cloner l'appareil ou saisir l'original nous permettrait d'avoir en notre possession toutes les preuves pertinentes, <b>car</b> cloner l'appareil copie tous les bits et on ne peut pas avoir plus d'information que ce qui est sur l'original.</p> <p><b><u>Règle de la meilleure preuve :</u></b></p> <p>La meilleure preuve est l'original. <b>Cependant</b>, cloner l'appareil offre la même valeur probante, <b>car</b> on copie à la fois les éléments irréels et réels. <b>Donc</b>, la preuve ne perd pas de qualité.</p> <p><b><u>Force minimale :</u></b></p> <p>Si on opte pour cloner, l'utilisation de la force est minimale, car Jean sera en mesure de continuer de faire usage du téléphone.</p> <p>Si on opte pour saisir l'original, l'utilisation de la force n'est pas minimale, <b>car</b> Jean ne sera pas en mesure de faire usage du téléphone. <b>Cependant</b>, il a lui-même affirmé ne pas s'en servir fréquemment, alors l'impact n'est pas aussi élevé que si c'était son téléphone personnel.</p> <p>Il y a utilisation de la <b>force par privation de jouissance</b>, <b>car</b> l'appartement de Jean Saies est occupé par les investigateurs.</p> <p>Il y a utilisation de la <b>force psychologique</b>, <b>puisque</b> Jean Saies ne sait pas si nous allons être en mesure de trouver des preuves sur son cellulaire. Il peut <b>donc</b> se sentir stressé ou craintif d'être poursuivi. De plus, il peut ressentir un inconfort face à l'invasion de sa vie privée, puisque le cellulaire contient des photos personnelles.</p> <p><b><u>Intrusion minimale :</u></b></p> <p>L'intrusion n'est pas minimale, <b>car</b> Jean est présent tout au long de la perquisition. Il est privé de son matériel, <b>car</b> il ne peut pas utiliser son cellulaire pendant la perquisition (ou pendant un temps indéterminé si on opte pour la saisie de l'original).</p> <p>Il y a une intrusion dans sa vie privée, <b>car</b> l'appareil contient des images personnelles qui peuvent avoir de la valeur sentimentale. De plus, certaines images sont particulièrement intimes et témoignent possiblement d'événements importants dans la vie de Jean. En effet, il y a une image d'une femme couchée dans un cercueil et si on présume qu'elle était la femme de Jean, cette image est hautement privée.</p> <p>Il y a une intrusion dans la vie privée de Jean <b>dû</b> au fait que la perquisition est dans son appartement, mais elle est minimale puisque Jean a utilisé son appartement comme un bureau de travail. Il a <b>ainsi</b> renoncé partiellement à sa vie privée à cet endroit.</p> <p>Il y a une intrusion minimale dans son cellulaire, <b>car</b> les mesures de protection et de contrôle misent en place sont minimales, <b>puisque'il</b> a choisi de ne pas le sécuriser à l'aide d'un NIP ou d'un mot de passe.</p>
---	---

## **Interruption minimale des opérations d'entreprise ou des fonctions domestiques :**

Les opérations de l'entreprise sont interrompues momentanément, **car** Jean est présent tout au long de la perquisition (il est un membre clef de l'entreprise).

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.gsmarena.com/samsung_galaxy_a8_(2018)-8886.php)

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