

## Formulaire TP Stratégie de fouille

Numéro d'équipe : B

Image E01 assignée : 6

Nom des équipiers :

(9) → 71,55 / 100  
Coéquipier #1 : Imad Berrahil 2169358

(10) → 72,55 / 100  
Coéquipier #2 : Ngaliako Hakoua Mauger 2159572

(10) → 72,55 / 100  
Coéquipier #3 : Yassine EL JAMALI 2165837

(9) → 71,55 / 100  
Coéquipier #4 : Simon Tran 1961278

Ce TP est corrigé sur 100 et compte dans le résultat final du trimestre pour la valeur indiquée au plan de cours. Les éléments suivants sont corrigés séparément du contenu du formulaire selon les critères indiqués :

- Formulaire {55 points} : La plupart des questions requièrent une réponse précise. Exemple : Un sous-numéro dont valant 1 point. Si la réponse correcte est « .docx » et que vous répondez « .doc », ça vaudrait ½ point. Si vous répondez « .jpg » ça vaudrait 0 point. Pour les questions à développement (exemple du numéro 3 ci-dessous), la réponse est évaluée en fonction de la qualité argumentatoire.
- Contenu des pièces à conviction originales (ad1) {10 points} : Présence ou absence. Divers autres critères.
- Contenu des pièces à conviction converties {10 points} : Présence ou absence. Divers autres critères.
- Notes manuscrites {10 points} : Pour cet item, le pointage est individuel. Numérisées et incluses dans un répertoire séparé du zip. Manuscrites et non prises à l'ordinateur. Horodatées. Identité de l'investigateur sur la première page. Initiales de l'investigateur sur chaque page. Prises à l'encore bleue. Concordent avec celles des coéquipiers. Lisibilité. Syntaxe compréhensible. Divers autres critères.
- Qualité du français {5 points} : Sans faute d'orthographe, syntaxe exempte d'imprécision, de tournure de phrase incorrecte, de formulation ambiguë, ponctuation correcte, pas d'anglicisme, pas d'usage excessif d'acronyme et tableau des acronymes. Divers autres critères.
- Médiagraphie {5 points} : Style uniforme, quantité d'entrées, format des citations correct. Divers autres critères.
- Appréciation du correcteur et respect des directives (cours et énoncé) {5 points} : Formatage du texte, qualité des arguments et motivations. Divers autres critères.

Le nombre de points maximum accordés pour une question se trouve entre accolades {}. Pour une sous-question, vous le trouverez entre parenthèses carrées [].

Vous devez respecter les indications de longueur de réponse lorsqu'il y en a. Ces indications sont de style « 1 à 5 mots » ou « 1 à 2 phrases ».

Le formulaire comme tel est déjà paramétré à 1½ interligne.

Les indications « Notez bien » sont là pour vous faire penser que certaines pièces à conviction doivent être versées au ad1 et converties. Mais ces indications ne couvrent pas 100% des pièces à conviction à joindre au ad1 et à convertir.

**Attention** : Le formulaire commence à la page 2. Veuillez ne pas modifier la mise en page. Si une question se trouve sur la page 4, faites en sorte qu'elle ne déborde ni sur la page 3 ni sur la page 5. MERCI d'aider à rendre la correction efficace.

### Rappels afférents à ce TP :

- Les décalages s'expriment en hexadécimales et comportent point de référence/décalage début/décalage fin (ou longueur).
- Sauf lorsqu'indiqué autrement, lorsqu'on demande une stratégie ou votre stratégie ou la stratégie, vous devez fournir un plan A **ET** un plan B.
- Lorsqu'on demande où vous avez trouvé votre preuve, vous devez divulguer le conteneur (fichier ou partition ou...) et décalage complet où on peut retrouver cette preuve.

### Résultats pour ce TP :

<u>Item</u>	<u>Points obtenus</u>	<u>Sur un max de</u>	<u>Commentaire</u>
Formulaire	44,75	55	
Contenu des pièces à conviction originales (ad1)	7,5	10	Signature?
Contenu des pièces à conviction converties	5,3	10	Crime désencastré? File slack? (A)
Notes manuscrites		10	
Qualité du français	3	5	
Médiagraphie	0	5	
Appréciation du correcteur et respect des directives	2	5	Non respect du format du zip
Total	62,55	90	

(A) Plan.docx et Word.docx doivent être  
arrangés avec la bonne extension

	Correcteur
<p>1) Signaturé {4 point(s)} : Quelle stratégie de fouille avez-vous utilisé pour trouver le fichier produit par le logiciel Signaturé (1 à 5 mots).</p> <p>1) Les stratégies utilisées : c'est par <u>Métadonnée-extension</u> ?</p> <p>2) Donnée-recherche par mot clé</p> <p><b>Notez bien</b> : N'oubliez pas de fournir ce fichier parmi les pièces à conviction ainsi que l'application Signaturé si elle se trouve sur la clé USB.</p>	2/4

<p>2) Fichier .rib {12 point(s)} :</p> <p><b>Notez bien</b> : N'oubliez pas de fournir le fichier .rib parmi les pièces à conviction, le fichier désencastré de ce fichier .rib et tous les fichiers constituant un crime similaire à celui illustré dans le fichier désencastré du .rib</p> <p>a) [1 point(s)] Que représente (quel crime) le fichier désencastré du fichier .rib? Utilisez les mots de l'énoncé de travail</p> <p>Sofa : Diffamation</p> <p>l'article 301 : D'écris qui Quiconque publie un libelle diffamatoire est coupable d'un acte criminel et passible d'un emprisonnement maximal de deux ans</p> <p>b) [2 point(s)] À l'aide de quelle stratégie de fouille avez-vous réussi à le désencastrer (exceptionnellement, ne fournissez qu'une seule stratégie)? (1 à 5 mots)</p> <p>Métadonnée-Signatures de fichiers</p> <p><del>début "FF D8 FF E0 " et de fin "FF D9 " =Format .jpg</del></p> <p>c) [3 point(s)] Donnez les coordonnées en système <u>sexagésimal</u> GPS indiquées dans ce fichier</p> <p>Selon la stratégie de fouille métadonnée- intradonnées on a pu extraire la localisation via l'application Geosetter (GeoSetter)</p> <p>N45°38'47.47"W74°57'0.43" ✓</p> <p>d) [3 point(s)] Répondez à la première question se trouvant dans les <u>intradonnées</u> du fichier</p> <p>Glaude Parisakys fut arrêté dans l'une des chambres de ce complexe hôtelier après y avoir retenu un employé contre son gré pendant 2 jours. Qui est le propriétaire de cet établissement hôtelier? Dans quelle localité se situe-t-elle?</p> <p>Fairmont le Château Montebello → ça c'est le nom de l'hôtel, mais qui en est le propriétaire?</p>	<p>①</p> <p>1/2</p> <p>③</p> <p>0/3</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------

<p>e) [3 point(s)] Répondez à la seconde question se trouvant dans les <u>intradonnées</u> du fichier</p> <p>Dans quelle <u>localité</u> se situe-t-elle? :</p> <p>On exploitant l'adresse trouvé avec Système GPS indiqué dans les intradonnées du fichier, on pu extraire l'adresse ci-dessous avec google Maps:</p> <p>392 Rue Notre Dame, Montebello, QC J0V 1L0</p> <p><i>Ne Répondez pas en dehors de la question</i></p>	<p>1.5/3</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------

<p>3) Cartes de crédit {7 point(s)} : Décrivez <u>succinctement</u> ce que vous avez comme preuve relative aux cartes de crédit</p> <p>Recherche par expression régulière : <math>(\backslash d\{4\}-)\{3\}\backslash d\{4\}</math> et une fouille par exploration du contenu recherche dans Arborescence dans la partition 1 nommé Aime2014 /root ,dans la liste des fichiers:</p> <p>Fichier1: Lac artificiel.JPG.FileSlack et Fichier2: Meuh!.JPG.FileSlack</p> <p><i>C'est quoi un FileSlack ?</i></p> <p>Nous avons retrouvé ces numéro de cartes de crédits lors de la fouille :</p> <table><tr><td>4505-4785-5557-1119</td><td>731</td><td>1/15</td><td>THOMAS</td><td>Nantel</td></tr><tr><td>5491-9150-3709-4319</td><td></td><td></td><td></td><td></td></tr><tr><td>4505-1322-4609-1029</td><td>709</td><td>12/11</td><td>DEAN</td><td>Kirouac</td></tr><tr><td>5491-5531-3074-7410</td><td>557</td><td>3/15</td><td>TALY</td><td>Perez</td></tr><tr><td>3790-193395-53133</td><td>2875</td><td>6/12</td><td>KEENAN</td><td>Bedard</td></tr><tr><td>3790-125259-68264</td><td>8970</td><td>6/15</td><td>ISAAC</td><td>Beauvais</td></tr><tr><td>3790-175132-41302</td><td>4767</td><td>3/11</td><td>NOLANN</td><td>Goupil</td></tr></table> <p>Recherche par stratégie de fouille par exploration du contenu recherche dans Arborescence avec Autopsy :/img_Image6/vol_vol4/ pop.googlemaile.com/ Inbox</p> <p>En fouillant dans les mails que M. Parisakys a envoyés, on trouve des preuves de trafic de cartes de crédit, toutes avec le même code NIP 8765. Mr. Parisakys explique qu'il les produit lui-même. Opération "Fleur-du-dessert".</p> <p>En testant le NIP des cartes ci-dessus retrouvées dans les dossiers personnels de Mr. Parisakys, cela constituerait une preuve de l'utilisation de cartes de crédit non réglementées.</p>	4505-4785-5557-1119	731	1/15	THOMAS	Nantel	5491-9150-3709-4319					4505-1322-4609-1029	709	12/11	DEAN	Kirouac	5491-5531-3074-7410	557	3/15	TALY	Perez	3790-193395-53133	2875	6/12	KEENAN	Bedard	3790-125259-68264	8970	6/15	ISAAC	Beauvais	3790-175132-41302	4767	3/11	NOLANN	Goupil	<p>6.5/7</p>
4505-4785-5557-1119	731	1/15	THOMAS	Nantel																																
5491-9150-3709-4319																																				
4505-1322-4609-1029	709	12/11	DEAN	Kirouac																																
5491-5531-3074-7410	557	3/15	TALY	Perez																																
3790-193395-53133	2875	6/12	KEENAN	Bedard																																
3790-125259-68264	8970	6/15	ISAAC	Beauvais																																
3790-175132-41302	4767	3/11	NOLANN	Goupil																																

- 4) Fichiers suspects {4 point(s)} : On vous demande de fournir, parmi les pièces à conviction, les fichiers correspondant aux empreintes numériques ci-dessous. Comment avez-vous procédé pour les trouver?

Nous avons utilisé une stratégie de fouille basée sur les données (empreintes numériques).

Deux méthodes sont possibles afin de réaliser cette stratégie de fouille. Nous avons utilisé extraction la liste des hash des fichiers depuis FTK Imager dans la partition2 puis rechercher ceux qui correspondent à notre liste.

Voici ci dessous la liste des empreintes numériques ainsi que le chemin vers le

**Fichier correspondant :**

**FTK Imager :** Image6/Partition2/HAIE2014 [FAT16]/root dans FTK Imager

Autopsy en important le hashset dans le module “hash lookup” puis nous avons regardé quels fichiers étaient retournés :

**Autopsy :** /img\_Image6/vol\_vol4/

Empreinte	chemin
740C153680F3C4C731C07F3823584C7F	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\fouilli.jpg
033CBF77367D0713C90BACA4BD993B31	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\Image.png.JPG
5E17C0B5190A3DD44559FCA866B05D38	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\pensée.jpg
DC2B269E7437EE2C4578BA2F69CA3AE9	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\plan.docx
32806B6D053B1A9490C7845ECD44E4AC	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\trappe.jpg
A0C92FC2BB9DCCDEE98BE3A34B218A8B	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\worbiln.zip
E34D4D9F1425AA2839AE32B722EA6DA7	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\zaczac.jpg
1DEBAF445AEE73A8D44D9F4B30DD871D	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\000arbrouj.JPG
73BF44076768585452D1253B38F13B9F	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\drudde.bmp
66A039AF41C3FB8D480DDC67E3440332	Image6\Partition 2 [23MB]\HAIE2014 [FAT16]\[root]\fleura.jpg

**Notez bien :** N’oubliez pas de fournir parmi les pièces à conviction les fichiers se rapportant au crime commis à l’endroit du fils de l’individu ayant accosté Parisakys au restaurant kiribatien

- 5) Algarade au restaurant {7 point(s)} :

- a) [2 point(s)] Quel est le nom du fils de l’individu ayant accosté Parisakys au restaurant kiribatien? 2 à 3 mots  
Côme Envatt-Uyaudepoêle

4

2

b) [1 point(s)] Quel crime cet individu lui reprochait-il? 1 phrase

“Crimes contre la personne, Voies de fait grave”

268 (1) Commet des voies de fait graves quiconque blesse, mutilé ou défigure le plaignant ou met sa vie en danger.

En effet, Parisakys a eu recours de manière intentionnelle à la violence physique envers un étudiant qui n'était pas consentant dans le but de l'intimider, jusqu'à causer sa défiguration. Ainsi nous suggérons l'article 268(1) à Marianne Fitzwalter.



1

c) [3 point(s)] Décrivez succinctement la preuve à cet égard

L'échange de mail de l'ami de Parisakys (TiPhonse) a demandé l'aide pour se venger de Côme puisqu'il a manqué de respect à l'égard de sa fille. Parisakys dans sa réponse au mail a confirmé qu'il a bien exécuté le crime comme montre les messages celle des échanges entre eux :

**Tiphonse :**

Peux-tu envoyer un gars pour donner des cours de bienséance au gars.

Il s'appelle Côme Envatt-Uyaudepoêle.

Dis-moi ce que je te dois.)

**Parisakys :**

J'ai décidé de m'amuser, histoire de faire un tour dans mon passé de jeune criminel. J'ai rencontré Uyaudepoêle sur le campus, devant sa classe de juste-bons-à-étudier. Quand je suis arrivé, il ressemblait à DiCaprio. J'y ai fourré toute une volée (j'avais mon poing américain et mes bottes à cap d'acier). Quand je l'ai lâché, y'était peu beau: j'ai pris sa photo et je l'envoie ci-jointe.

+ photo ?

2/3

d) [1 point(s)] Quelle stratégie de fouille vous a permis de trouver ces preuves? 4-5 mots

Stratégie utilisée: Exploration du contenu- Arborescence

1

**Notez bien :** N'oubliez pas de fournir, parmi les pièces à conviction, les preuves démontrant que Parisakys connaît, même si c'est de façon indirecte, ce que les Frères de l'Eau préparent

6) Les Frères de l'Eau {12 point(s)} :

a) [7 point(s)] Quel est le message des Frères de l'Eau?

Neptune, Mon Frère. Notre Déesse Frija, notre Sainte Mère nourricière, t'ordonne d'oeuvrer pour le bien-être de tes frères assoiffés. Les assoiffeurs québécois accumulent l'eau et nous refusent l'accès à leur richesse. L'eau est un trésor patrimonial international et tous ont droit d'y puiser ce qui est utile à leur survie. Si nous ne pouvons accéder à cette richesse, personne ne devrait pouvoir y accéder. Ta mission est donc de détruire ta cible et de faire passer le message que les Frères de l'Eau ne tolérerons plus qu'on refuse l'accès au Trésor mondial aux pauvres et aux déshérités. Si tu réussis, Frija Notre Mère te promet que tu passeras ta seconde vie dans l'eau pure et désaltérante. Que Frija te prenne dans ses bras et assure ta sécurité. Bziatga plegg Manis!.. 50°38'49.94"N. 68°43'36.01"O

7

b) [1 point(s)] Dans quel type de fichier avez-vous trouvé le message ? 3 lettres

PNG.

1

c) [1 point(s)] Quelle stratégie de fouille vous a permis d'extraire ce fichier d'où il était (exceptionnellement, ne fournissez qu'une seule stratégie) ? 1 à 5 mots

Métadonnées -intradonnées en utilisant exiftool

1

d) [3 point(s)] Que vous fait craindre ce message ? 1 ou 2 phrases

Ta mission est donc de détruire ta cible et de faire passer le message que les Frères de l'Eau ne tolérerons plus qu'on refuse l'accès au Trésor mondial aux pauvres et aux déshérités. Ce message nous fait craindre un attentat qui a pour but de détruire un édifice (en décodant l'adresse du message on obtient N50°38'49.94"W68°43'36.01" qui pointe sur un barrage ou la Centrale de Manic 5 à Québec).

3

7) Code postal {3 point(s)} :

a) [1 point(s)] Quel est le code postal de Parisakys? Code postal seulement : 6-7 caractères

Le code postal de Parisakys : H2O-2A7

b) [2 point(s)] Quelle stratégie avez-vous employé pour le trouver? Soyez précis et détaillé, mais succinct

Dans les échanges de mail nous avons vu que Parisakys semble habiter au Canada,

nous avons donc utilisé le format d'un code postal au Canada afin de réaliser une

stratégie de fouille basée sur les données (expression régulière). Nous avons donc

utilisé l'expression régulière suivante : ([A-Z]\d[A-Z]\d[A-Z]\d).

Si cela n'avait pas fonctionné, nous aurions pu élaborer une stratégie de fouille

basée sur les données, en allant consulter les mails échangés.

①

**Notez bien** : N'oubliez pas de fournir, parmi les pièces à conviction, les preuves démontrant les agissements criminels de Parisakys et de ses collaborateurs

8) Complices {6 point(s)} :

Donnez le nom des complices de Parisakys et le crime dans le(s)quel(s) il(s) collabore(nt)

Complices	Crime
Parisakys - Akaraboudjan (TiPhonse)	268.Voies de fait graves + SC
Parisakys -Robert devereux (Roberto)	342.B) falsifie une carte de crédit ou en fabrique une fausse;

5/6



**Notez bien** : N'oubliez pas de remettre vos notes **manuscrites** d'investigation numérique avec votre rapport. Celles-ci doivent être photographiées ou numérisées puis incluses dans le fichier ad1 soumis avec ce formulaire. Elles ne doivent donc pas être mises en annexe du présent rapport. Ces notes **ne peuvent pas** être des notes prises à l'ordinateur.