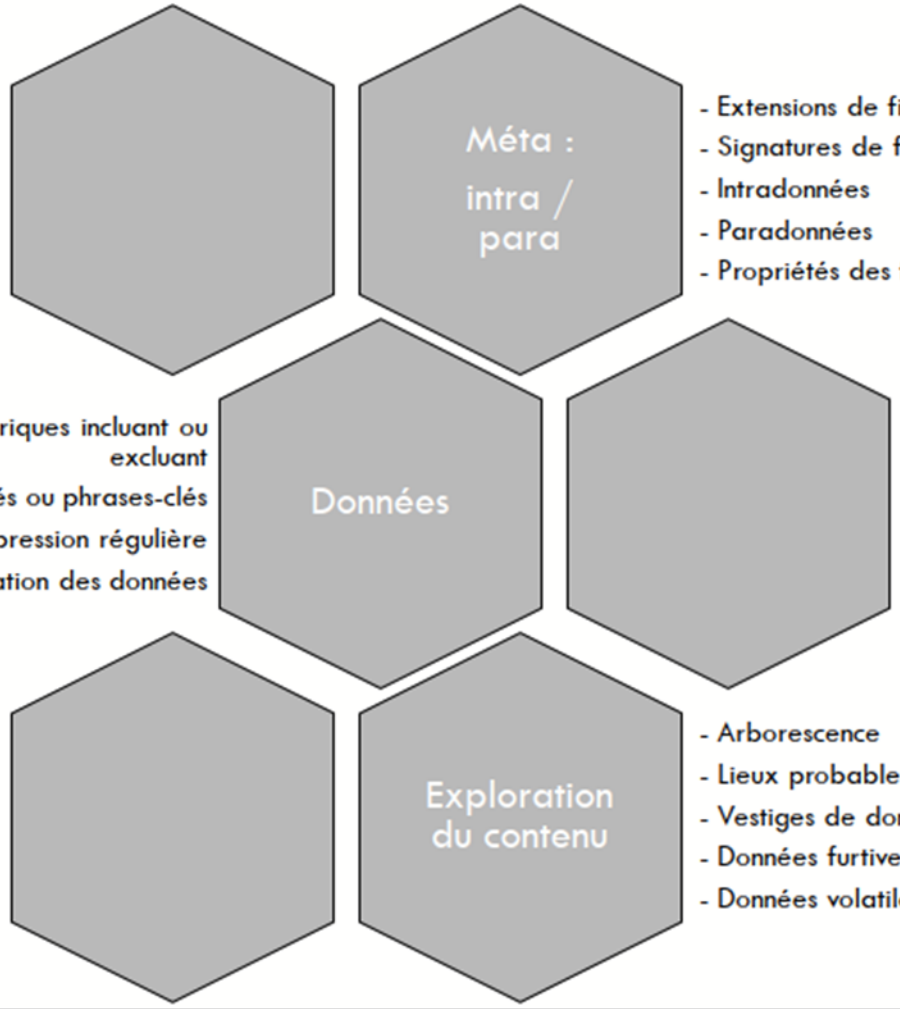
INVESTIGATION NUMÉRIQUE – STRATÉGIES DE FOUILLE

IFT3002 (UL), 8SEC202 (UQAC) ET INF8430 (POLYTECHNIQUE)

Pensez double!

STRATÉGIES DE FOUILLE ET D'EXAMEN



DIAPOSITIVE #63 (2 stratégies même si pas demandées comme telle)

- Stratégie
- Source (+façon de l'obtenir)
- Outil pour appliquer
- Cible et méthode d'application
- Résultats escomptés
- Utilisation projetée

COMPRENDRE LA QUESTION

- Famille de stratégie – Stratégie: Tel que dans le manuel. N'inventez rien!
- Source: C'est-à-dire l'intrant que vous utiliserez dans la stratégie. Exemples:
  - Le mot-clé que vous utiliserez et d'où il vient
  - L'expression régulière et ce qu'elle comporte (pas l'exprég comme telle mais sa structure)
  - La signature et où vous allez la prendre
  - L'extension et comment vous allez la trouver
- Outil pour exécuter la stratégie

COMPRENDRE LA QUESTION

- Cible: Ce sur quoi vous allez appliquer la stratégie, l'artefact dont vous voulez tirer des informations, l'artefact que vous fouillez. Exemples:
  - Le fichier dans lequel vous recherchez l'information
  - Le disque dur du suspect
  - Le téléphone cellulaire
- Méthode d'application: Comment vous allez vous y prendre pour utiliser l'application et exécuter la stratégie. Sommairement mais suffisamment

COMPRENDRE LA QUESTION

- Résultats escomptés: Quelles sont les données que vous espérez obtenir, l'extrant attendu, ce que vous pensez que la stratégie va pondre
- Utilisation projetée: On s'entend qu'une réponse comme « Obtenir des preuves de la culpabilité du suspect » est une lapalissade, n'est-ce pas? Vous devez faire plus pour avoir tous vos points et dire en quoi la donnée obtenue prouve la culpabilité du suspect. Par exemple: « Je veux démontrer que le suspect avait l'intention de frauder la victime en démontrant qu'il possédait les outils pour la tromper, car mon résultat est un fichier fabriqué par le logiciel d'impression de cartes de crédit »

CONCLUSION

- J'ai coupé de moitié le nombre de questions de stratégies à répondre
- Je serai plus exigeant sur la correction à l'examen
- N'OUBLIEZ PAS: de fournir stratégie A ET stratégie B même si on ne le demande pas spécifiquement. En effet, votre client ne vous demandera jamais « Quel est ton jeu de stratégies? ». Il vous demandera plutôt comment vous allez vous y prendre. Habituez vous donc à penser en double toujours

Interception de courriel d'un employé par un autre employé de la compagnie. L'intercepteur « s'amuse » à envoyer des courriels aux contacts de son collègue pour l'embarrasser

- Stratégie A: Données – Exploration de contenu
- Source: La victime me donne accès au contenu de son ordinateur afin que je puisse examiner les entêtes des courriels
- Outil pour appliquer: FTK Imager. La victime utilise un système de messagerie utilisant un format de fichier lu par mon logiciel de lecture de fichier de courriel
- Cible et méthode d'application: Disque dur de la victime monté en lecture seule sur mon laptop de fouille. J'extrais le fichier de courriel. Je le lis avec mon logiciel de lecture de courriels.
- Résultats escomptés: Recueillir une série de mots-clés et de phrases-clés
- Utilisation projetée: Pouvoir appliquer efficacement la stratégie B qui suit.

Interception de courriel d'un employé par un autre employé de la compagnie. L'intercepteur « s'amuse » à envoyer des courriels aux contacts de son collègue pour l'embarrasser

- Stratégie B: Données – Mots-clés ou phrase-clé
- Source: La victime, par la stratégie A.
- Outil pour appliquer: Autopsy
- Cible et méthode d'application: Disque dur du suspect monté en lecture seule sur mon laptop de fouille. Je lis le contenu des boîtes de courriel.
- Résultats escomptés: Trouver des courriels écrits par le suspect sur son ordinateur mais en utilisant l'accès de la victime
- Utilisation projetée: Démontrer que le suspect a, en sa possession, les courriels délictueux. Restera à déterminer que c'est lui qui les a écrit et envoyés