

Sommaire

[1. Contexte du TP 1](#_Toc133487243)

[2. Découverte du fichier .img 2](#_Toc133487244)

# 1. Contexte du TP

Une clef USB a été interceptée par notre équipe terrain.

L'origine de la clef est inconnue mais nous pensons qu'elle contient des données sur une prochaine attaque terroriste sur un site sensible.

Vous devez nous fournir un rapport détaillé sur le contenu de la clé :

* Localisation du Site Ciblé
* Localisation du Bâtiment Ciblé
* Date et Heure de l'attaque
* Origine de l'attaque

Nous pensons aussi que la clef a servie aussi pour installer un logiciel malveillant sur des postes sensibles :

Nous souhaitons avoir des informations sur :

* Type de logiciel malveillant
* Indices de Compromission
* Mode d'exécution

Nous comptons sur la qualité de votre rapport pour que nous puissions prendre les bonnes décisions pour contrer cette offensive.

Durée : 4h

La note portera à la fois sur les indices collectés à 25%, la méthode d'analyse 25% et sur la qualité du rapport 50%

# 2. Découverte du fichier .img

**/ ! \ Attention : Avant de commencer toute manipulation il convient d’installer une machine virtuelle isolée de notre réseau et de travailler dedans afin d’éviter tous problème sur notre machine physique. Dans l’énoncé nous voyons que la clé USB contient potentiellement un logiciel malveillant.**

Ouverture de l’image :