Challenge de Cybersécurité !!!

Contexte :

Dans ce défi, vous incarnez un "expert" en informatique forensique chargé de prouver qu'un employé d'une entreprise revend des informations aux concurrents.

Mise en situation

Vous êtes Gilbert Descloux, expert dans le domaine de l'informatique forensic. La société Sowaaa SA, un des leaders mondiaux sur le marché de sécurité des logiciels, a fait appel à vos services. Apparemment, ils suspectent un de leurs employés de vendre des informations à la concurrence.

Voici le mail que le responsable informatique de Sowaaa SA vous a envoyé:

Subject: Demande d'analyse concernant le poste 042
From: Raoul Jugnot <raoul.jugnot@sowaaa.com>
*Date: **Thu, 16 Dec 2015 14:44:36 GMT***
To: Gilbert Descloux <gilbert.descloux@hotmail.com>

Monsieur Descloux,

Suite à nos précédents mails, nous avons décidé de vous confier cette affaire. Nous suspectons l'utilisateur du poste 042 de fournir des informations à nos concurrents. C'est pourquoi, lundi, nous avons capturé le trafic réseau sortant et entrant de son poste de travail. Nous avons également effectué un backup de sa partition /home.

Votre travail sera de déterminer si effectivement il fait sortir certaines informations de l'entreprise. Et si c'est le cas, trouvez à qui il a fourni quels informations et comment.

Les fichiers concernant l'employé sont en pièces jointes de ce mail.

En espérant que ces informations suffiront, je vous souhaite bonne chance. Tenez nous au courant de votre avancement.

--
Raoul Jugnot
Responsable informatique
Sowaaa SA

Votre objectif

Votre mission sera d'aider ce pauvre Gilbert Descloux. Il y a plusieurs informations clés à découvrir. Le but final est de savoir quels documents ont étés vendus et ce qu'ils contenaient.

Pour ce faire vous disposez d'une image de la partition *home* faite avec la commande *dd*. Pour vous faciliter la tâche, après une analyse préliminaire, on a trouvé deux mails échangés entre l'employé et une personne d'un concurrent de l'entreprise Sowaa SA. Cependant, rien de spécial dans ces mails, les deux personnes avaient échangé quelques photos qu'ils les ont prises pendant leurs vacances.

Le mail en provenance d'un contact extérieur :

Date: Sun, 13 Dec 2015 14:40:22
From: Hubert Trébuchet <hubert.trebuchet@free.fr>
To: Jean Delafourchette <jean.delafourchette@sowaaa.com>
Subject: Photo de vacances

Salut Jean !
Voilà la photo dont je t'avais parlé la dernière fois. J'aime beaucoup la tour Eiffel à Paris.

Bonne semaine,
Hubert

Pièce jointe : Tour-Eiffel.jpg

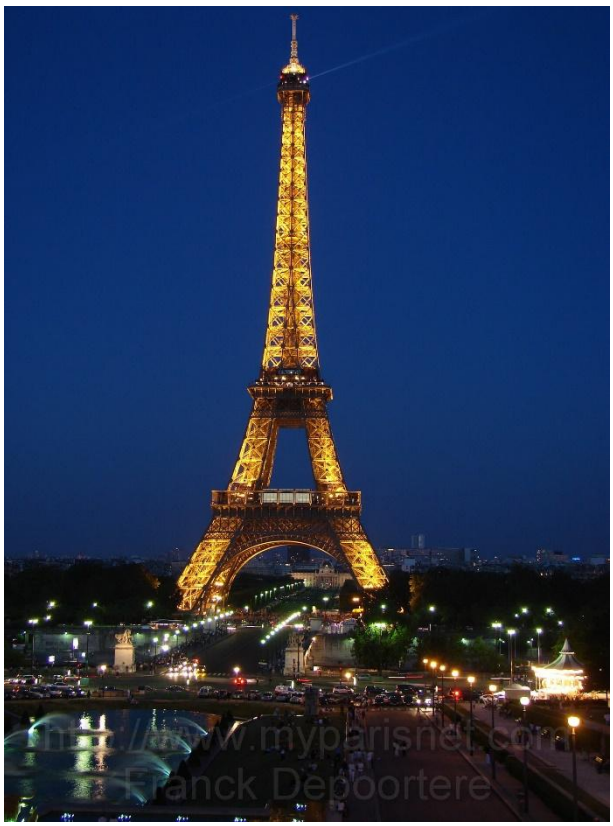

Figure 1. Tour-Eiffel.jpg

Le mail sortant :

Date: Sun, 13 Dec 205 15:16:36
From: Jean Delafourchette <jean.delafourchette@sowaaa.com>
To: Hubert Trébuchet <hubert.trebuchet@free.fr>
Subject: Photo de vacances

Salut Hubert !

Je suis de retour des USA. J'étais à New York. J'ai bien reçu ton message, merci. Je t'envoie deux petites photos que j'avais prises sur le pont de Brooklyn et le statue de la liberté à New York. J'aime beaucoup le pont de Brooklyn et le Statue.

A une prochaine,
Jean

Pièces jointes : Brooklyn_Bridge.jpg et Statue.jpg

Figure 2.Brooklyn_Bridge.jpg

Figure 3. Statue.jpg

Travail à réaliser :

1. On soupçonne que ces mails contiennent des secrets, la première chose à vérifier et de voir s'il y a des données sensibles dans ou sur ces images. On pense à la stéganographie !! Tester avec l'outil *steghide* (à télécharger avec apt-get) pour vérifier si les images cachent-elles des informations.
2. On soupçonne que dans la figue 1, Hubert avait envoyé un secret que Jean l'a utilisé. Quel est ce secret ? quelle est sa nature ? Vérifier l'heure d'envoi du mail.
3. Jean a-t-il envoyé des données sensibles à Hubert ?

A utiliser

- La classe Java BigInteger
- La classe Java GregorianCalendar

Ex :
Pour générer un nombre aléatoire, on utilise souvent le temps de l'ordinateur. Pour plus d'information, voir la classe Java GregorianCalendar. Cette classe est utilisée pour générer des nombres aléatoires pour les éléments cryptographiques comme DH, El Gammal, etc.

```
GregorianCalendar gc2=new GregorianCalendar(2015,11,13,14,33,0);
long l1=gc1.getTimeInMillis();
```

- Utiliser l'outil Steghide