TP 1

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

Scenario:
Vous êtes Elliot Hackerman, un expert dans le domaine de l'informatique forensique. NotThatEvilCorp, l'un des leaders mondiaux du marché des logiciels, avait besoin de vos services. Apparemment, ils soupçonnent l'un de leurs employés de vendre des informations à la concurrence.

Voici le mail que le IT Manager de NotThatEvilCorp SA vous a envoyé:

Subject: Demande d'analyse du poste de travail 042
From: Sam Sung <Sam.sung@notthatevilcorp.com>
Date: Jeudi, 16 Dec 2015 14:44:36 GMT
To: Elliot Hackerman <elliot.hackerman@myOwnBoss.com>

Monsieur Hackerman,
Suite à nos précédents emails, nous avons décidé de vous confier ce dossier. Nous soupçonnons l'utilisateur du poste de travail 042 (un développeur **Java**) de fournir des informations à nos concurrents. C'est pourquoi, nous vous envoyons (ci-joint) la sauvegarde stockée de la partition /home de ce poste de travail.
Votre travail consistera à déterminer s'il fait réellement ressortir certaines informations de l'entreprise.
En espérant que ces informations suffiront, je vous souhaite bonne chance. Tenez-nous informés de vos progrès.

Sam Sung,
IT manager,
NotThatEvilCorp SA

Mission:
Votre mission sera d'aider ce pauvre Sam Sung. 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 créée avec la commande dd. Pour vous faciliter la tâche, après une analyse préliminaire, nous avons trouvé deux courriels échangés entre l'employé et une personne d'un concurrent de NotThatEvilCorp SA. Cependant, rien de spécial dans ces emails, les deux personnes venaient d'échanger quelques photos qu'elles avaient prises pendant leurs vacances.

L'e-mail du contact extérieur est:

Date: Dimanche, 13 Nov 2015 14:40:22
From: James ZeroZeroSix <James.zerozerosix@WeAreTheCompetitorsCorp.com>
To: Paul Suspected <paul.suspected@notthatevilcorp.com>
Subject: Photo de vacances

Salut Paul,
Ci-joint la photo dont je vous ai parlé, la dernière fois. J'aime beaucoup la Tour Eiffel à Paris.

Passe un bon moment,
James,

Pièce jointe: Eiffel.jpg

Figure 1. Eiffel.jpg

Le mail sortant :

Date: Samedi, 6 Dec 2015 15:16:36 GMT
From: Paul Suspected < paul.suspected@notthatevilcorp.com >
To: James zerozerosix < James.zerozerosix@WeAreTheCompetitorsCorp.com >
Subject: RE: Photo de vacances

Bonjour James,
Je suis de retour des USA. J'étais à New York. J'ai reçu votre message, merci. Je vous envoie deux petites photos que j'ai prises sur le pont de Brooklyn et la Statue de la Liberté à New York. J'aime beaucoup le pont de Brooklyn et la Statue de la Liberté.

Amicalement,
Paul

Pièces jointes:
Brooklyn_Bridge.jpg and Statue.jpg

Figure 2.Brooklyn_Bridge.jpg

Figure 3. Statue.jpg

Indices:

- Java class *BigInteger*
- Java class *GregorianCalender*

```
GregorianCalendar gc1=new GregorianCalendar(2020,06,14,09,33,0);
long l1=gc1.getTimeInMillis();
gc1.setTimeZone(TimeZone.getTimeZone("GMT"));
```

Afin de générer un nombre aléatoire, en Java, nous pouvons utiliser le temps de l'ordinateur comme une graine (« seed »). Pour plus d'informations, consultez la classe Java GregorianCalender. Cette classe est utilisée pour générer des nombres aléatoires pour des éléments cryptographiques comme DH, El Gammal, etc.

Bonne chance ☺