sekoia
#CYBERSECURITY

Guide utilisateur final FastIR Collector

FastIR Collector

Version : 1.0

06/01/2016

Public

SEKOIA - 16, Place de la Madeleine - 75008 PARIS
Tél. : 01 44 43 54 13 - Fax : 01 47 23 68 14 - E-mail : contact@sekoia.fr

www.sekoia.fr

Sommaire

1. Binaire

Actuellement, toutes les versions depuis Windows XP (en 32 ou 64 bits) sont supportées par FastIR Collector.

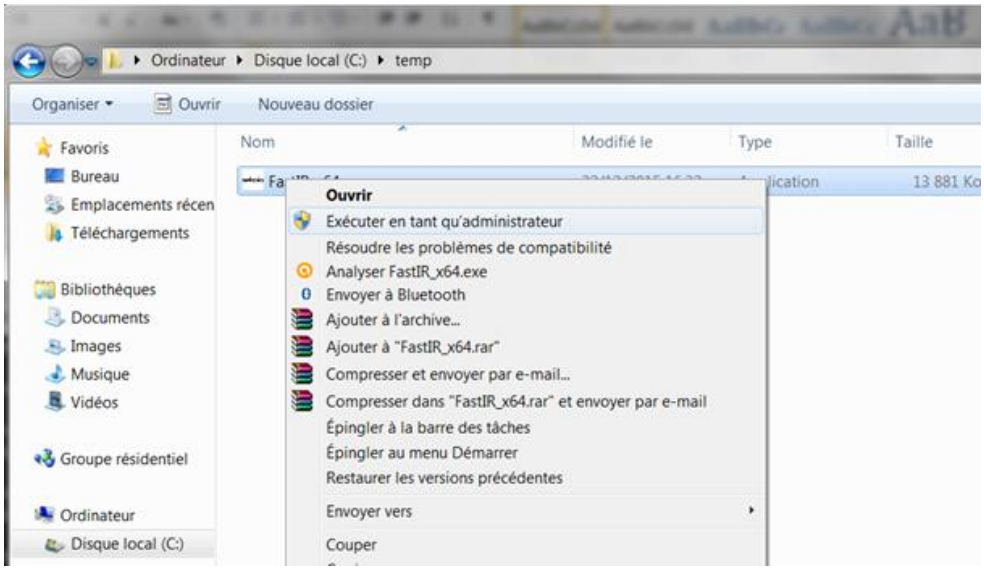
Les binaires sont disponibles sur le GitHub SEKOIA à l'adresse suivante : https://github.com/SekoiaLab/Fastir_Collector/tree/master/build

2. Guide utilisateur

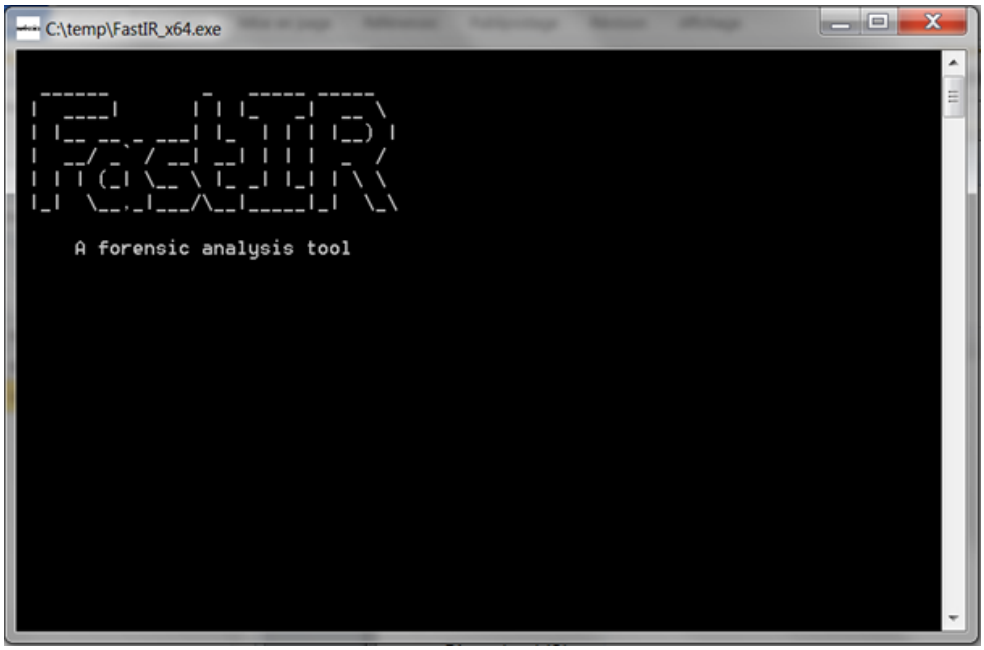
FastIR Collector nécessite des droits administrateur pour collecter l'ensemble des éléments nécessaires à l'analyse.

De ce fait, sous Windows Vista et supérieur :

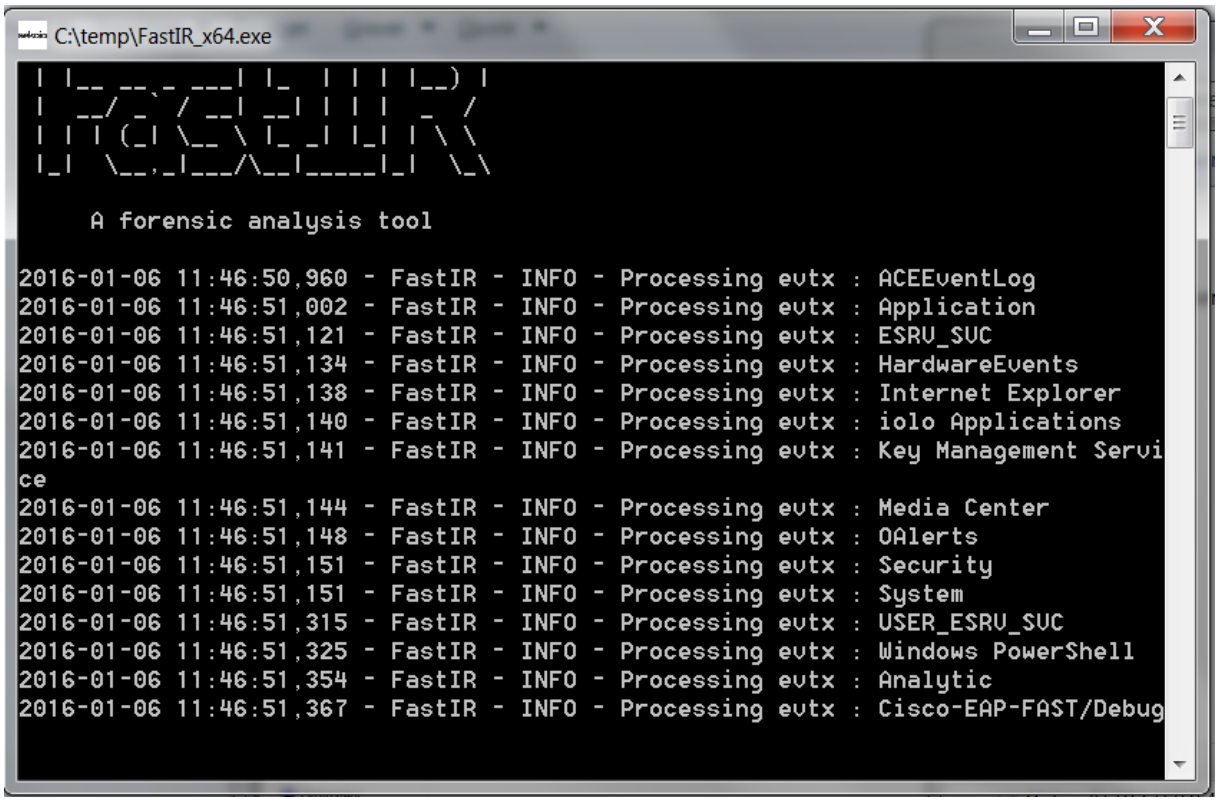
1- Dans le répertoire contenant l'exécutable, effectuez un clic droit sur **FastIR_x64.exe** et sélectionnez « **Exécuter en tant qu'administrateur** »



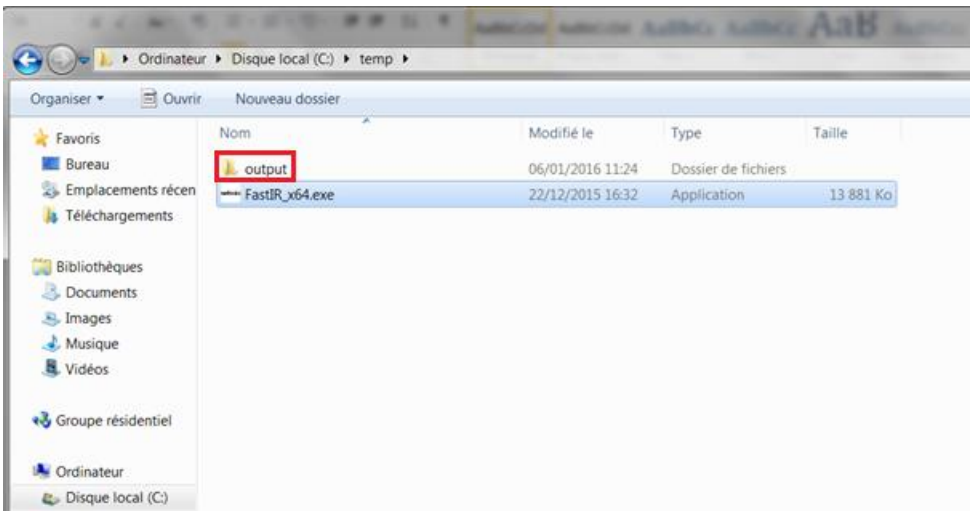
Une invite de commande se lance :



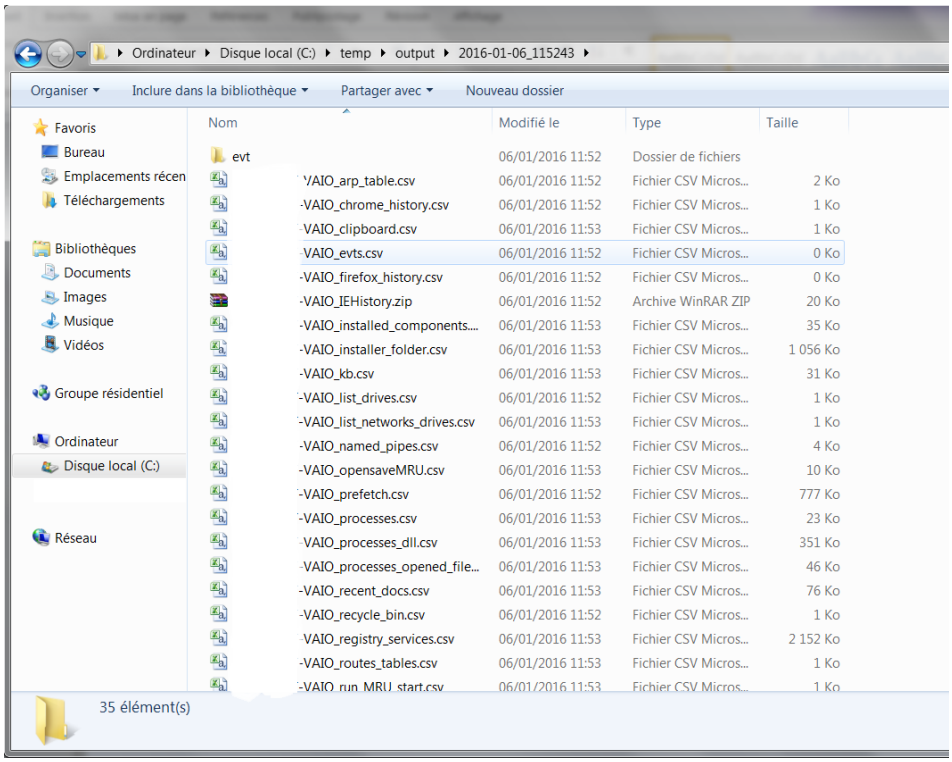
Puis la collecte démarre affichant un suivi de l'avancement des éléments collectés :



Au bout de quelques minutes, l'invite de commande se ferme et un nouveau répertoire nommé **output** apparait dans le répertoire contenant le binaire de FastIR Collector :

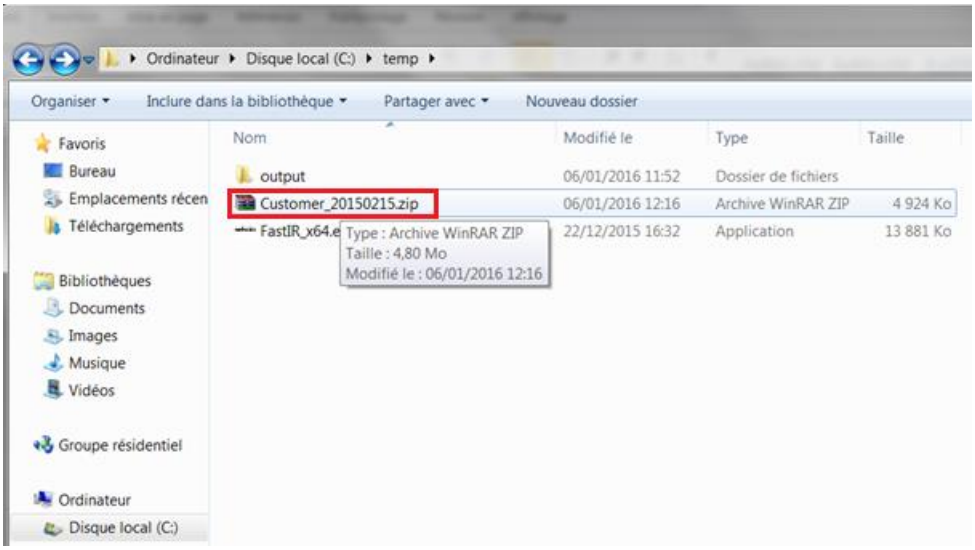


Si la collecte s'est déroulée correctement, on doit trouver dans le répertoire **output** un répertoire avec la date et l'heure de lancement de l'exécutable contenant un certain nombre de fichiers :



Si trois éléments seulement sont présents dans ce répertoire, c'est que l'exécutable a été lancé sans les droits d'administration.

2- Une fois les éléments collectés à l'aide de FastIR Collector, compressez le répertoire **output** à l'aide d'un utilitaire comme 7-zip :



3- Envoyer, par mail chiffré, le fichier compressé à l'adresse mail du CERT SEKOIA (cert@sekoia.fr).

3. Chiffrement des échanges avec le CERT

Pour chiffrer votre message avec GPG, **téléchargez la clé du CERT SEKOIA** depuis le serveur SKS (https://hkps.pool.sks-keyservers.net/pks/lookup?op=get&search=0x741E73BBB2317527)

User ID : CERT Sekoia
Key ID : B2317527
Fingerprint : 3B8C 4856 2B01 B4EF 0D04 C0C9 741E 73BB B231 7527

Cette méthode de communication est privilégiée.

Si GPG n'est pas supporté, le chiffrement S/MIME peut être utilisé. Il faut au préalable procéder à l'échange d'autorités de certification (root CA) afin de les ajouter dans les autorités de confiance. Ensuite, l'envoi d'un email au CERT SEKOIA est nécessaire pour effectuer l'échange de clés.

Enfin, le dernier moyen est de chiffrer le fichier compressé soit l'aide d'un utilitaire de compression (ex. : 7-ZIP), soit avec des logiciels de chiffrement (ex. : AxCrypt), puis de l'envoyer par mail. Le mot de passe devra être communiqué par un canal différent de celui utilisé pour l'envoi du message chiffré (ex. : par téléphone ou SMS).