sekoia
#CYBERSECURITY

FastIR Collector end user guide

FastIR Collector

Version: 1.0

01/06/2016

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

Summary

1. Binary

At the moment, every versions of Windows since Windows XP (both 32 and 64 bits) are supported by FastIR Collector.

The binaries are available on the GitHub of CERT SEKOIA at the following address:

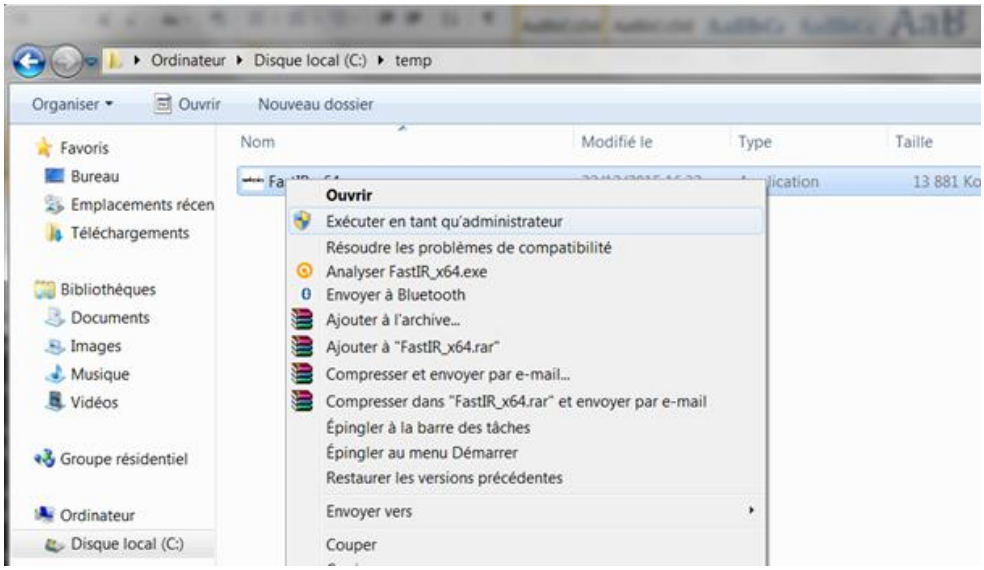
https://github.com/SekoiaLab/Fastir_Collector/tree/master/build

2. End user guide

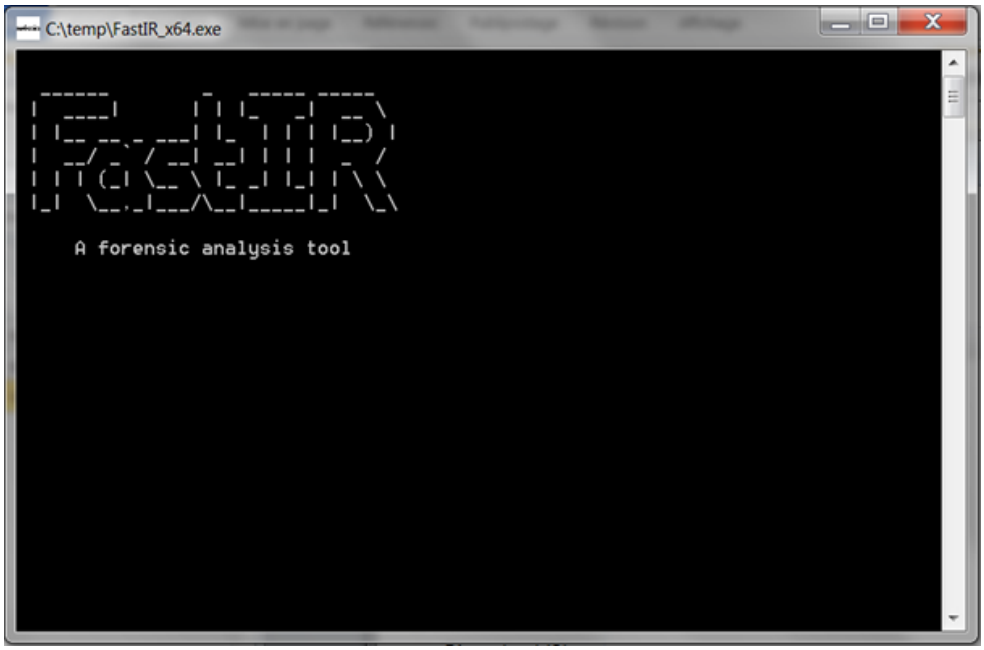
FastIR Collector requires administrative rights in order to collect all the necessary elements for the analysis.

As such, on Windows Vista and above:

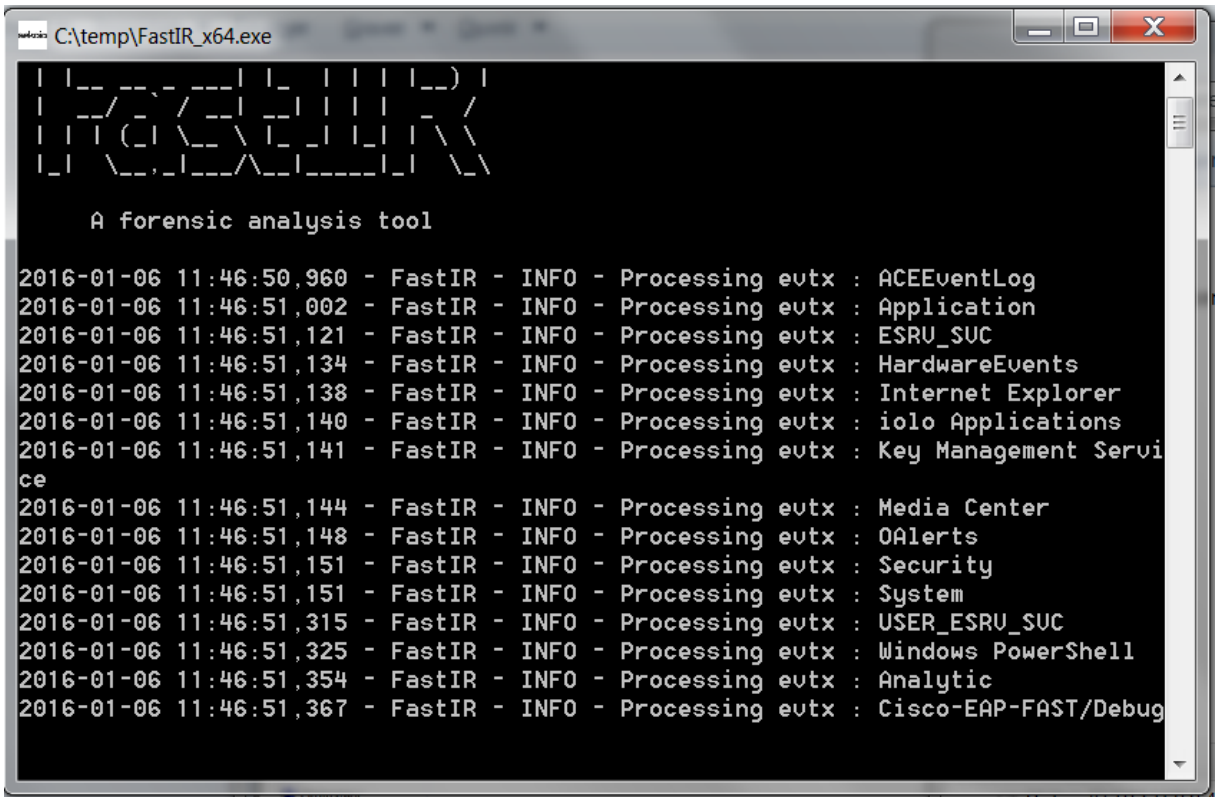
1- In the same directory containing the binary, right clic on **FastIR_x64.exe** and select "Run as administrator"



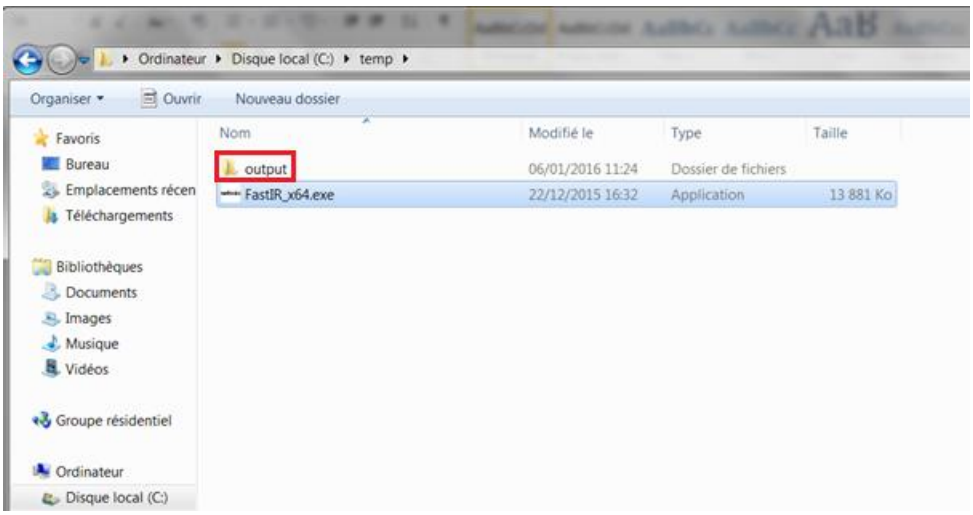
A command prompt appears:



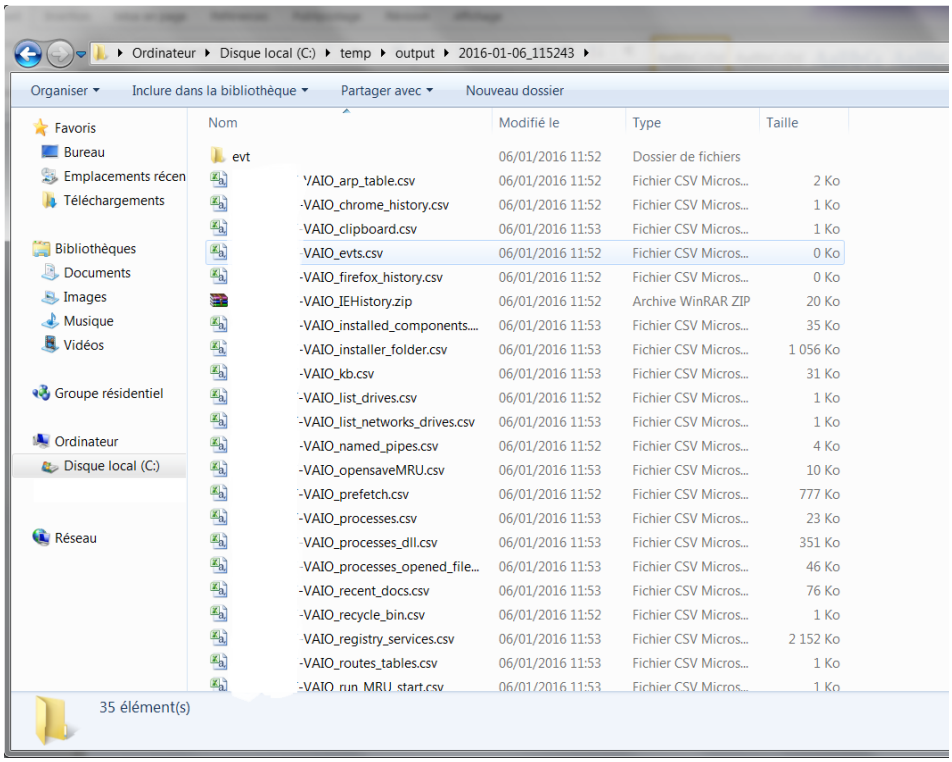
It then starts the collection, printing the status of the collection process:



After a few minutes, the command prompt automatically closes and a new folder called **output** appears in the folder containing the FastIR Collector binary:

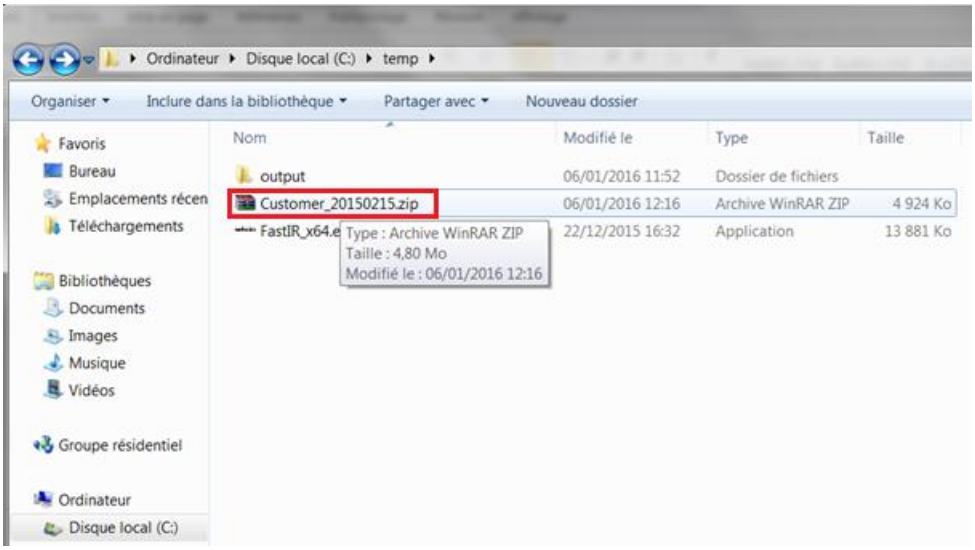


If the collection successfully completes, the **output** folder should contain another folder called "<DATE>_<HOUR>" of the execution. It contains several files:



If only three elements appear in this folder, it means the binary has not been executed under administrative rights.

2- Once all the elements have been collected, compress the **output** folder using a program such as 7-zip:



3- Send the compressed file in an encrypted email at cert@sekoia.fr.

3. Encryption of communications with the CERT SEKOIA

In order to encrypt the message using GPG, **download the public key of the CERT SEKOIA** from the SKS server at the following address:

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

This is the preferred way for communications.

If GPG is not supported, the S/MIME functionality can also be used. Each side first needs to accept the root CA of the other side. Then, an email exchange needs to be done in order to exchange signatures.

Finally, the archive can also be encrypted using password-protected archives (using 7-zip for example) or encryption software such as AxCrypt. The password should then be sent using another channel such as phone calls or SMS.