

diGiSignedOrProtectedPDF

Install Instructions – V1 – 2017.10.02

Step 0

Check the required Autopsy version: version 4.4.1

Step 1

- Copy the main two files of the module to the python_modules directory
- The two main files of the module are:
 - o **diGiSignedOrProtected_PDFs.py**: source code
 - o **SignedPDFs_Settings.db3**: SQLite DB to keep the settings

Step 2

The module depends on two external tools: **JSigPDF** and **ExifTool**.

- Install the JSigPDF application (<http://jsigpdf.sourceforge.net>)
- Install the ExifTool application (<https://sno.phy.queensu.ca/~phil/exiftool/>). Regarding ExifTool, make sure that the executable is named exiftool.exe (rename it, if needed).

Step 3

- First time the module is ran, it needs to be properly configured. Specifically, the “verifier EXE” and “exiftool EXE” fields need to be filled in with:
 - o The full path of **Verifier.exe**. (Verifier.exe is a program that exists in JSigPDF.). Under Windows 10, by default, Verifier.exe is in the **C:\Program Files (x86)\JSigPdf** directory¹.
 - o The full path of **exiftool.exe**.

Figure 1 highlights (yellow background) the fields that need to be filled in.

¹ Note that **verifier.exe** depends on the existence of some JAVA libraries and JAVA runtime in the directory where it is installed.

After having filled in the fields, do not forget to click **“Save Settings”** to have the fields persistently saved in the SQLite database. When the settings have been successfully saved, the message changes to **“OK – settings saved”** (Figure 2).

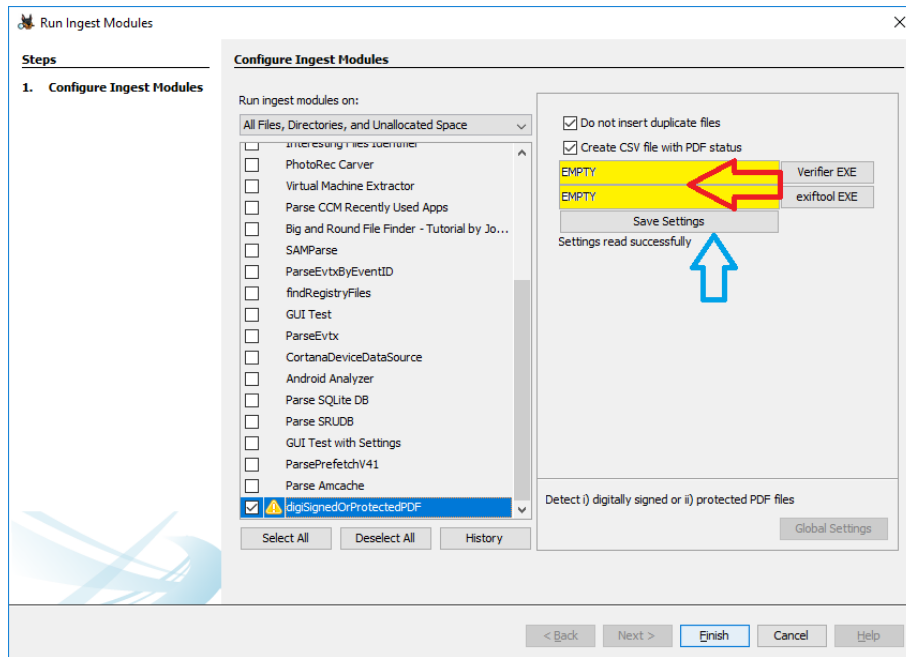


Figure 1

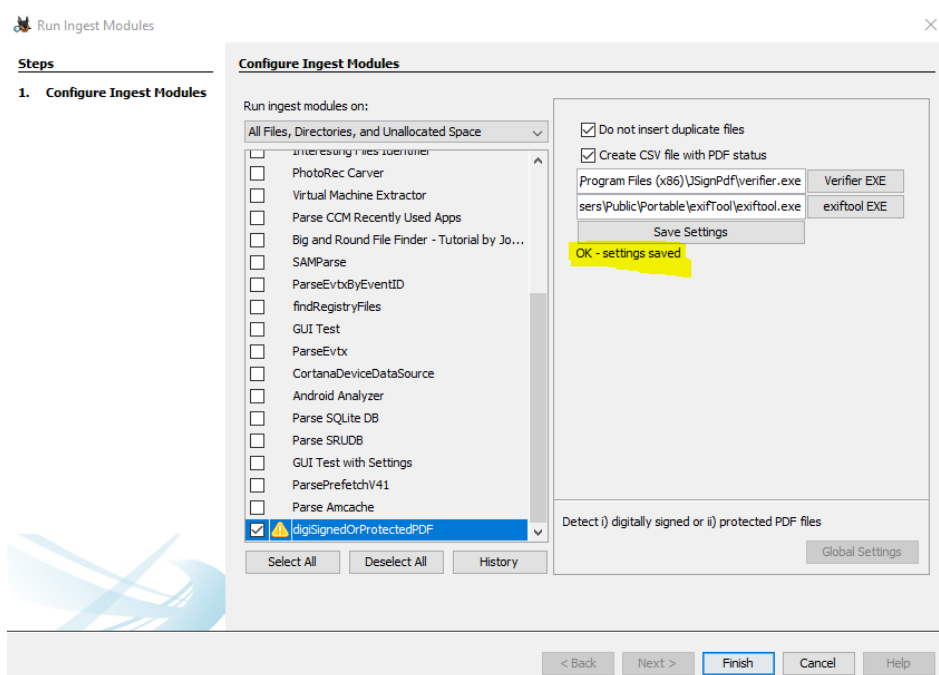


Figure 2

Step 4

- The module is now ready to be run (Figure 3)
- When done, the results are shown under the “**Interesting Items**” results tree (Figure 4)
 - o AssembleOFF_ModifyOFF: PDF files that have both properties disabled
 - o AssembleON_ModifyOFF: PDF files that have MODIFY property OFF, but ASSEMBLE on
 - o AssembleOFF_ModifyON: PDF files that have ASSEMBLE property OFF, but MODIFY on
 - o SIG_STAT_*: PDF files that are digitally signed. The signature might have some minor issues that are reflected on the name of the field (e.g., SIG_STAT_CODE_WARNING_NO_TIMESTAMP_TOKEN)
- If ordered to do so (CREATE CSV file with PDF status) , the module creates CSV files with the list of **digitally signed** files and another CSV files with the list of **protected** files.
 - o The CSV files are created in the **SignedPDFs** directory located in the **OutputFolder** of the autopsy case being analyzed.

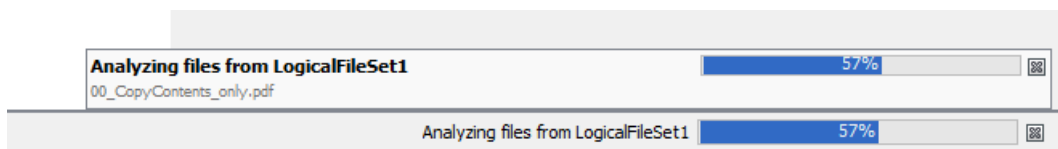


Figure 3

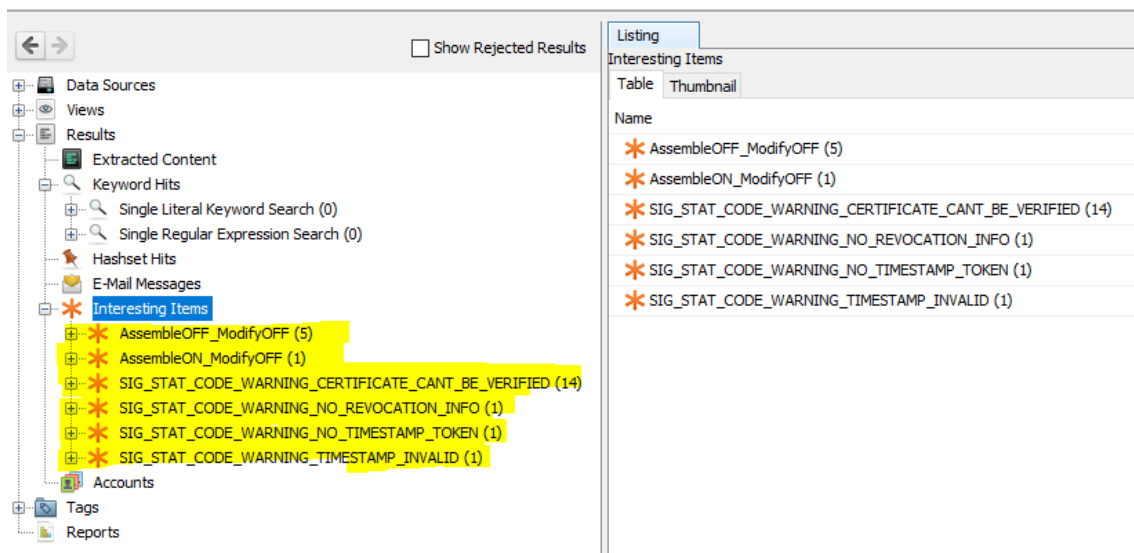


Figure 4