Forensic Emula Analyzer Manual (V1.0)

Forensic Emule Analyzer carves unallocated clusters of EnCase Image Files (*.e01) mounted with Access Data`s FTK Imager for deleted known.met records.

It recursively searches and parses active know.met files too.

FEA analyzes the internal structure of files and so it works with corrupted or partial files which crash some of the other known.met parsers.

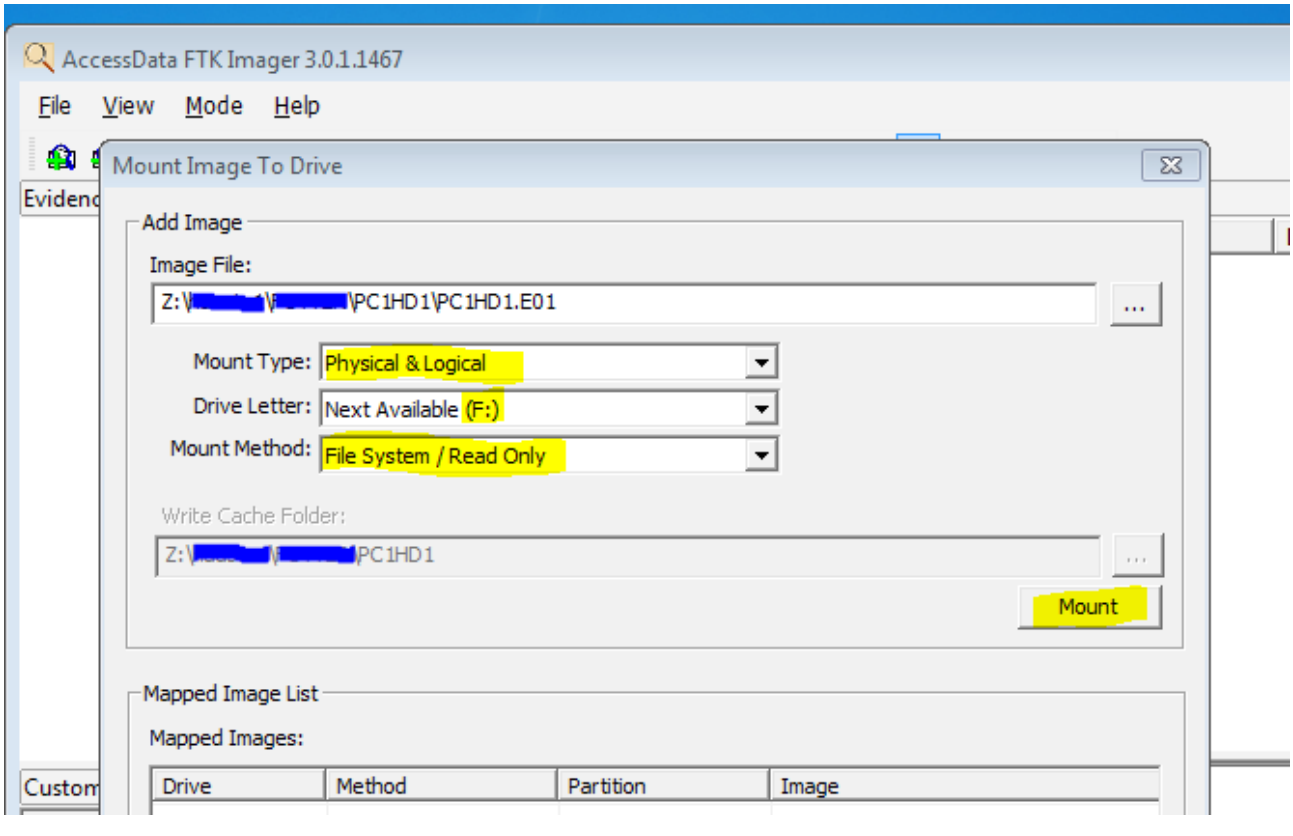
Forensic Emule Analyzer tries to write the parsed filenames as utf-8. If this fails it will write the filename byte by byte.

Questions, bug reports, success stories and feature requests mail to

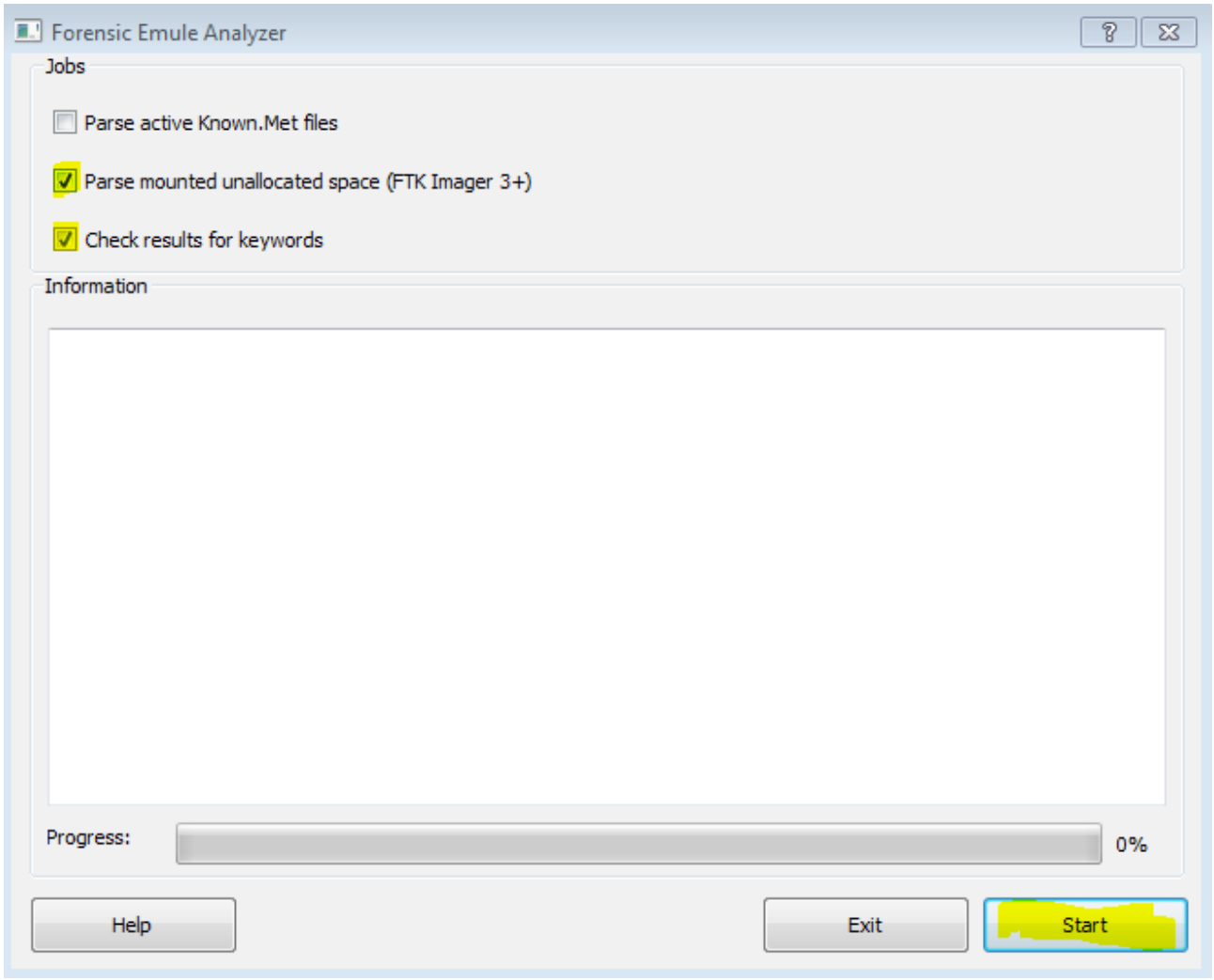
hexbugsandrocknroll@gmail.com

Carve known.met entries from unallocated spaces

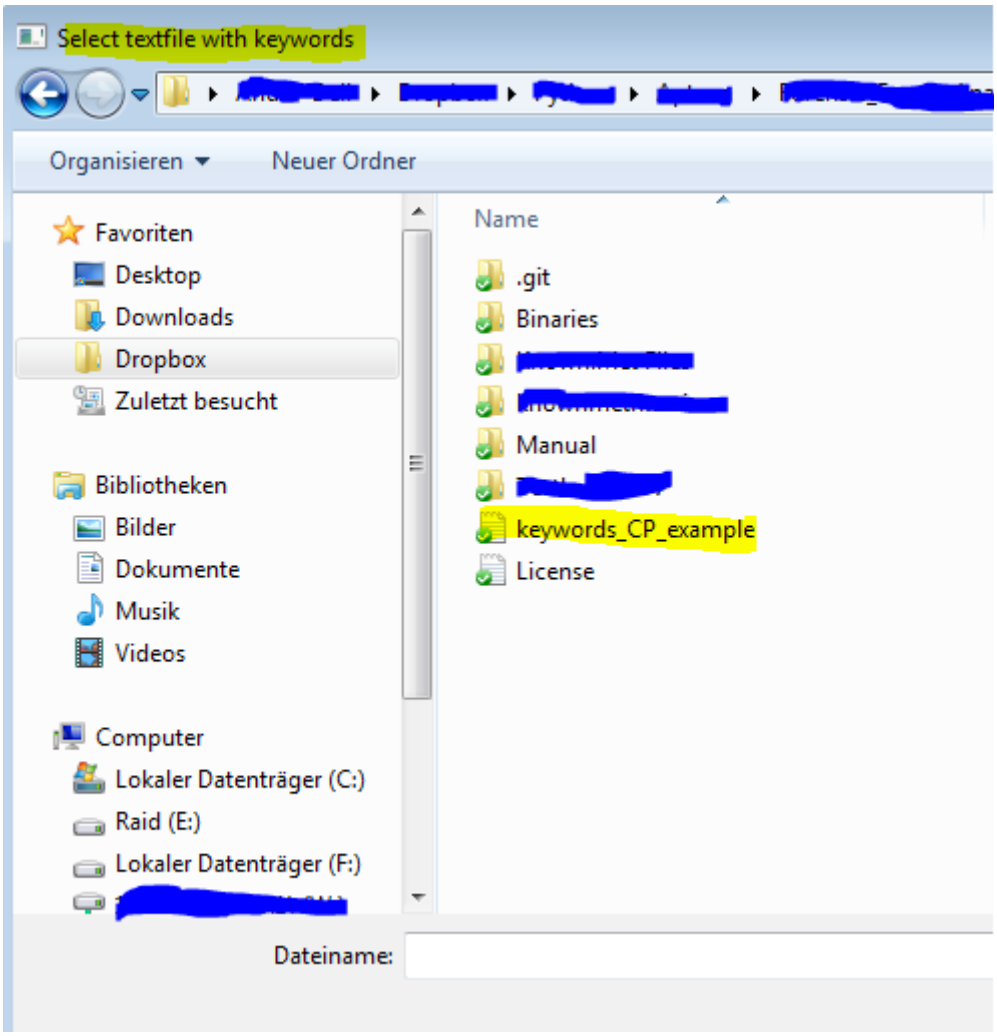
1) Mount the evidence (*.e01) using FTK Imager with the following settings. Note the drive letter (in this exampe F), you will need it later.



2) Start Forensic Emule Analyzer and select „Parse mounted unallocated space“ and „Check results for keywords“ (if you want to check the found filenames against keywords, eg. CP slang). Press „Start“ when ready.

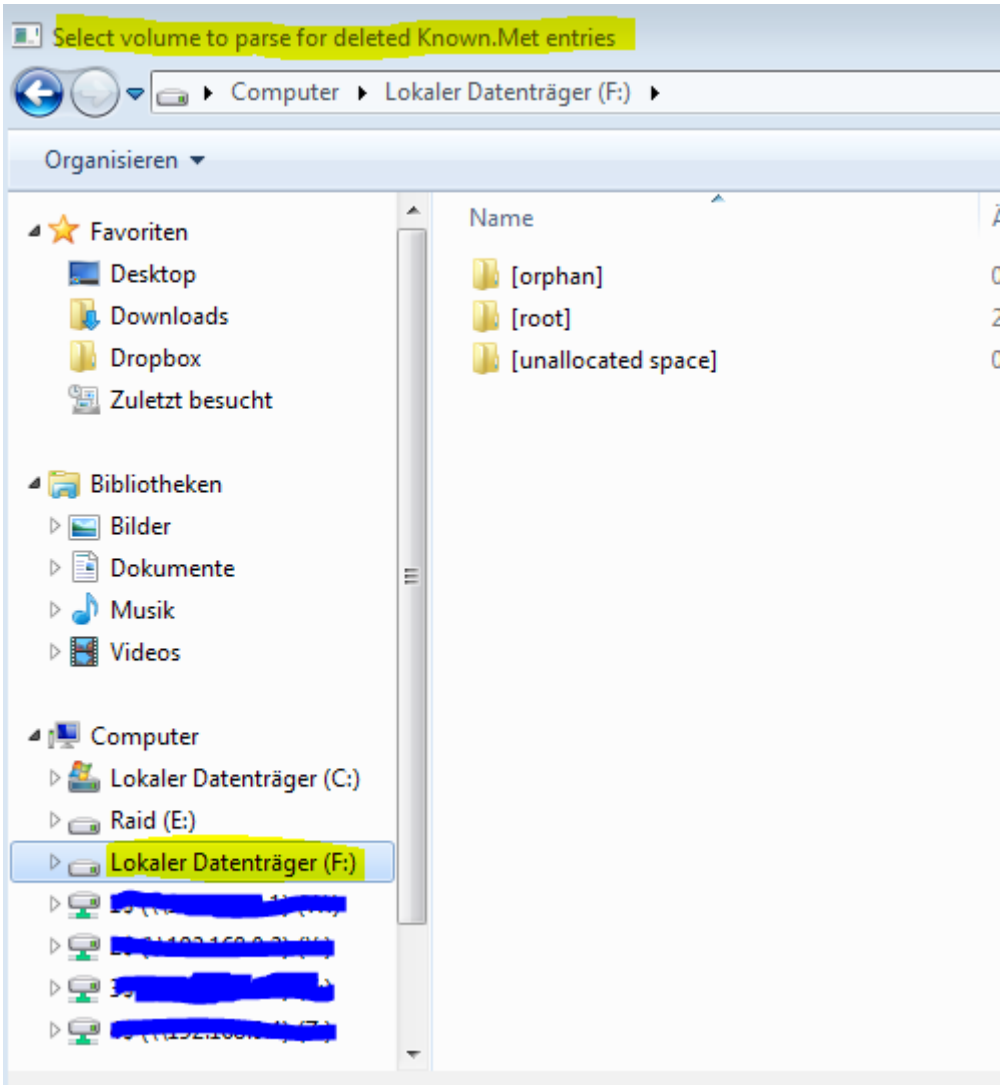


3) Select the file with the keywords. An example keywordsfile ist attached. Read it for more information how to compose a keywordsfile. Use a decent editor like notepad++.

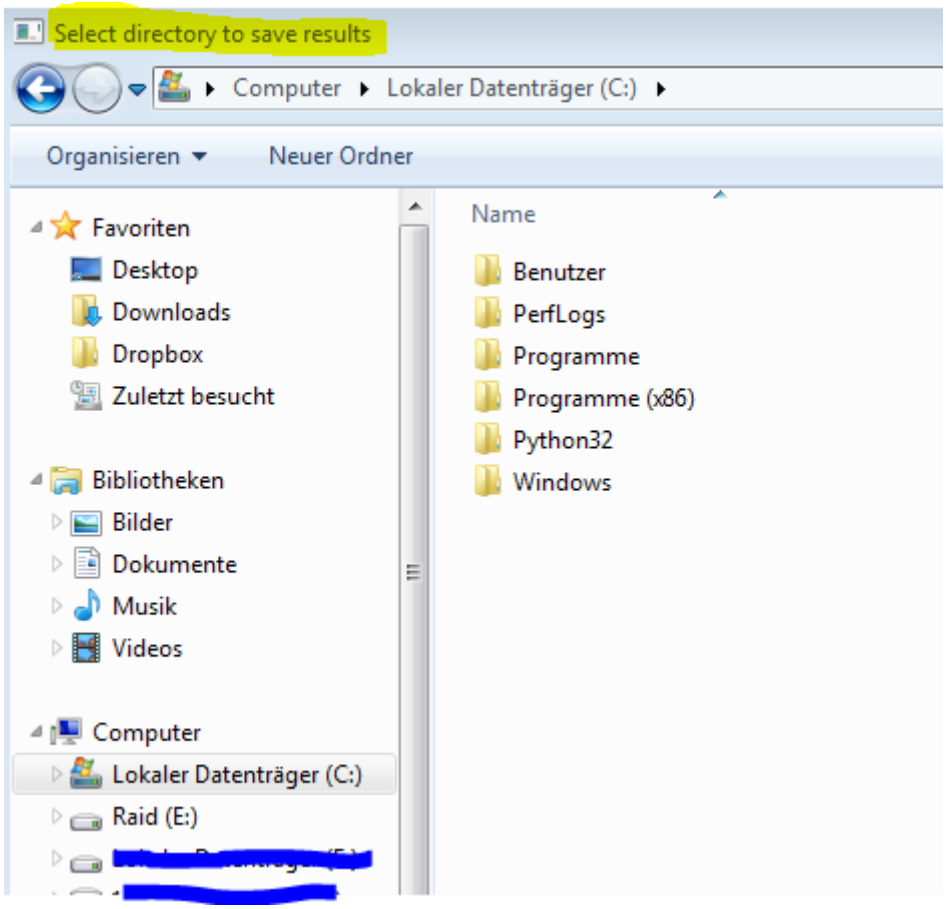


4) Select the volume to carve for deleted known.met entries. This is the drive letter from step 1.

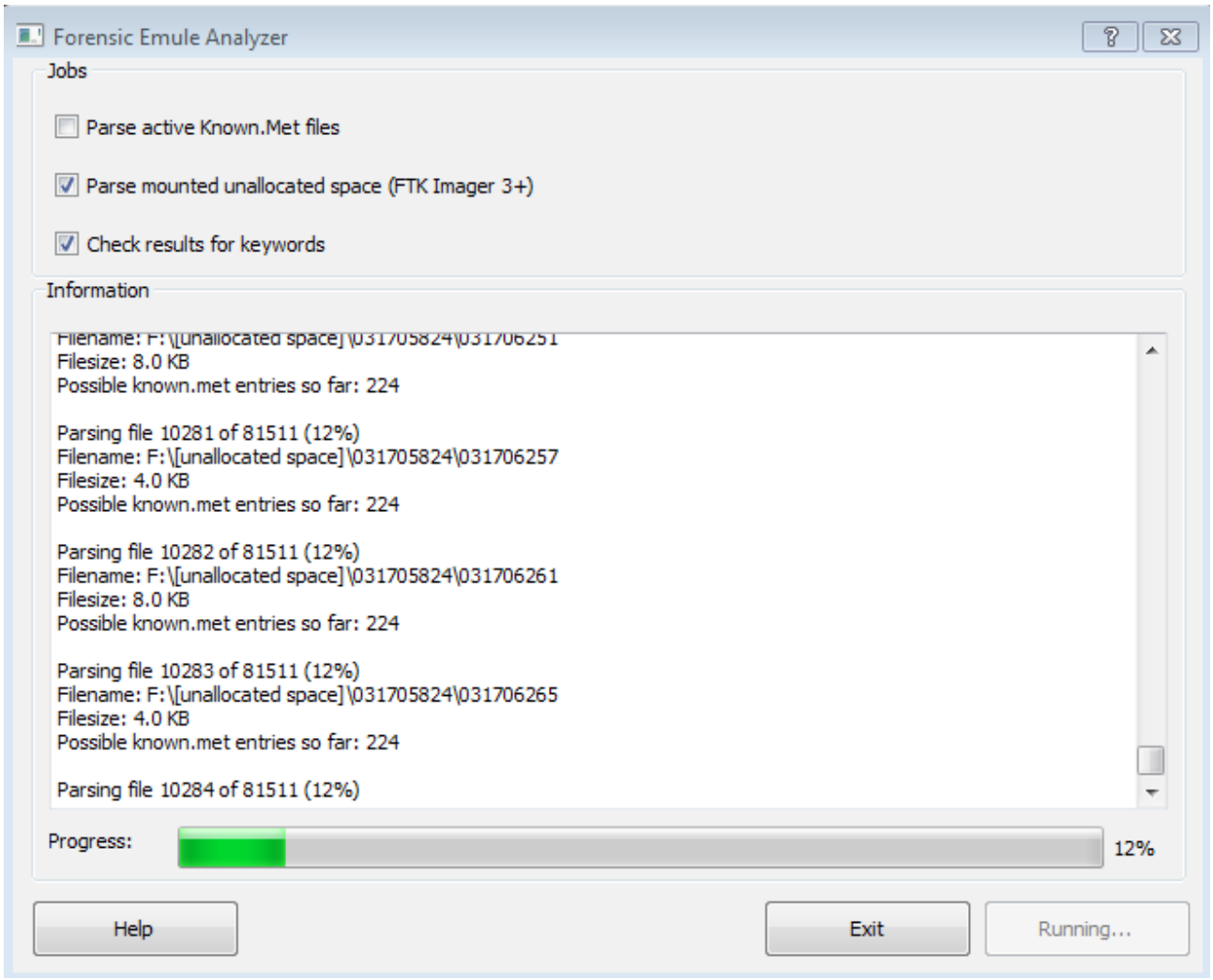
Important: Select „F:“ and not “F:\[unallocated space]“



5) Select the folder for the results.



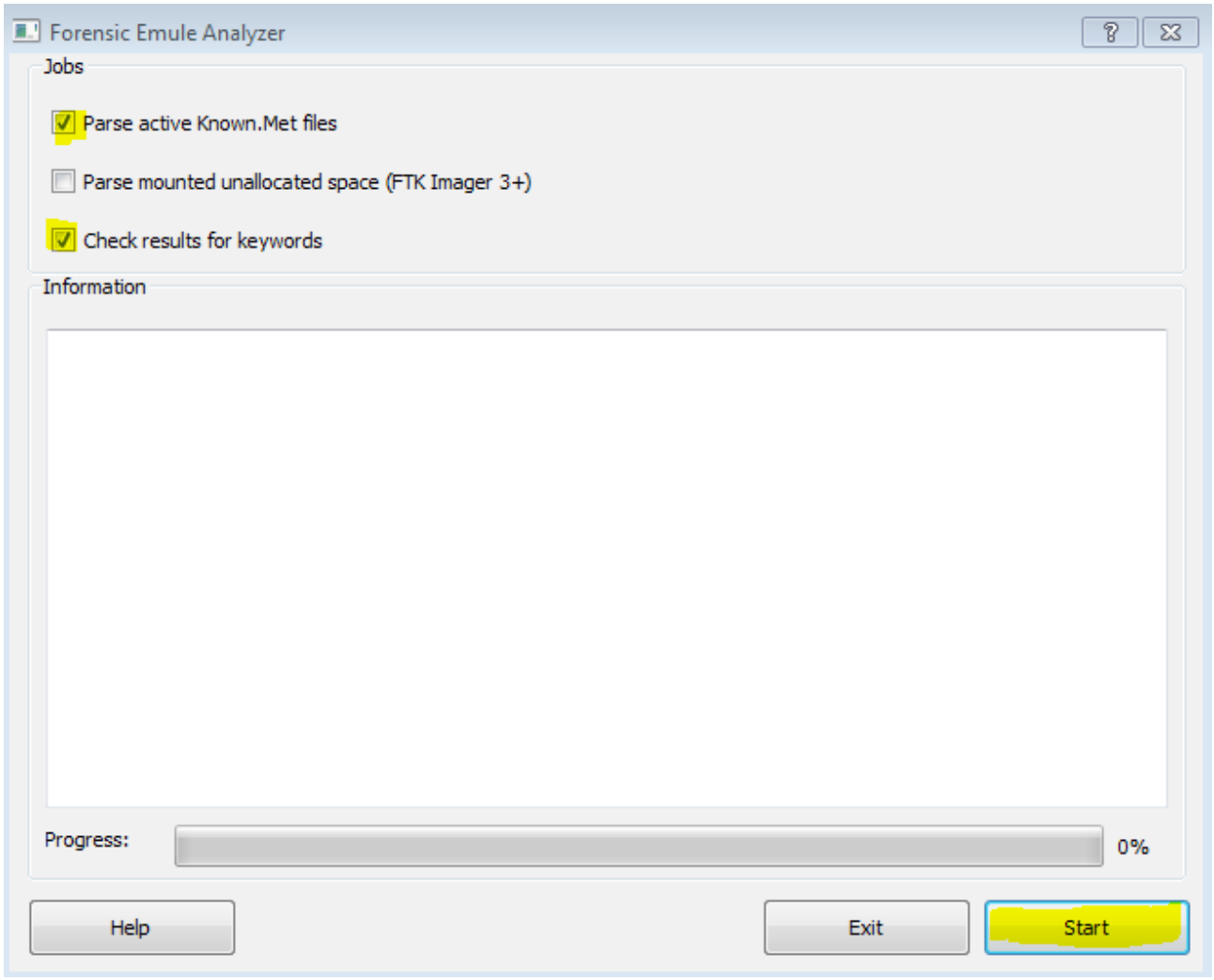
6) Forenisc Emule Analyzer gathers information about the unallocated spaces (this can take some time, be patient) and starts to carve known.met entries out of them.



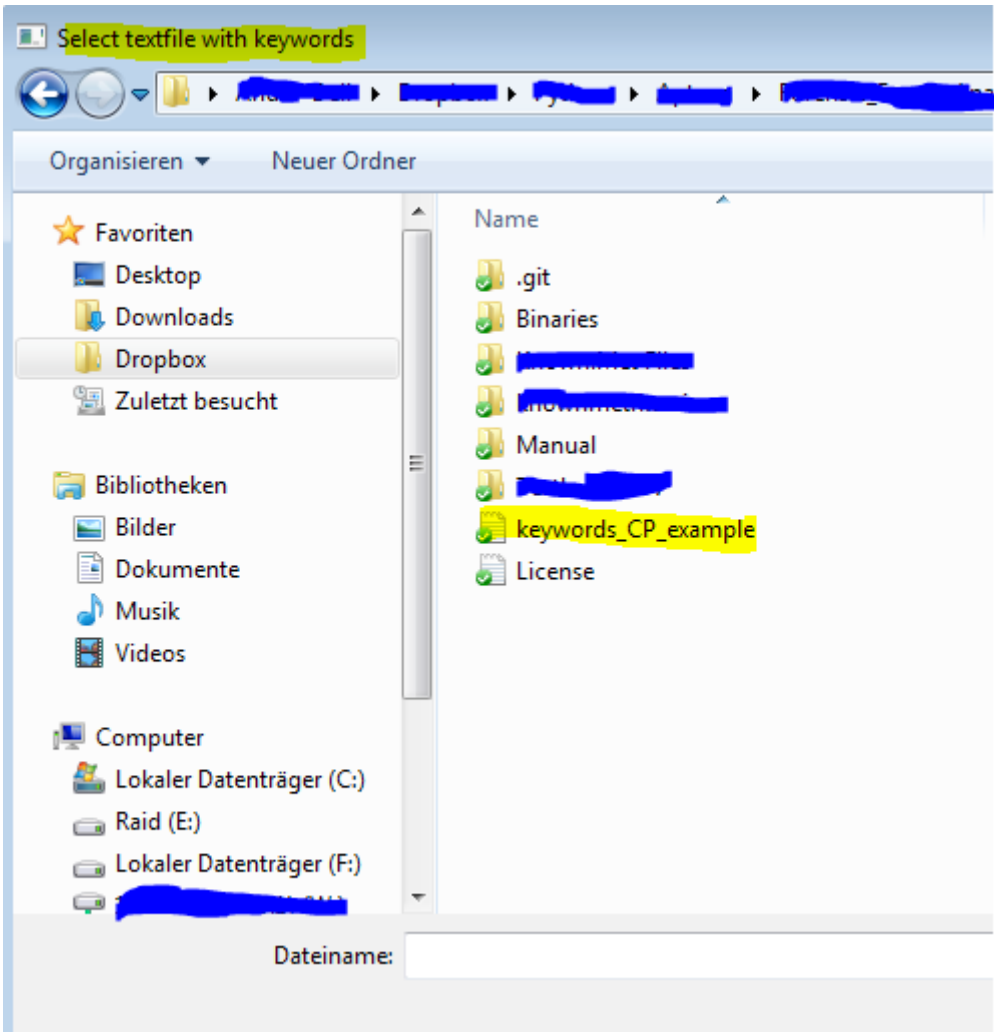
Parse active known.met files

To recursively search for aktive known.met files an analyze them, execute the following steps:

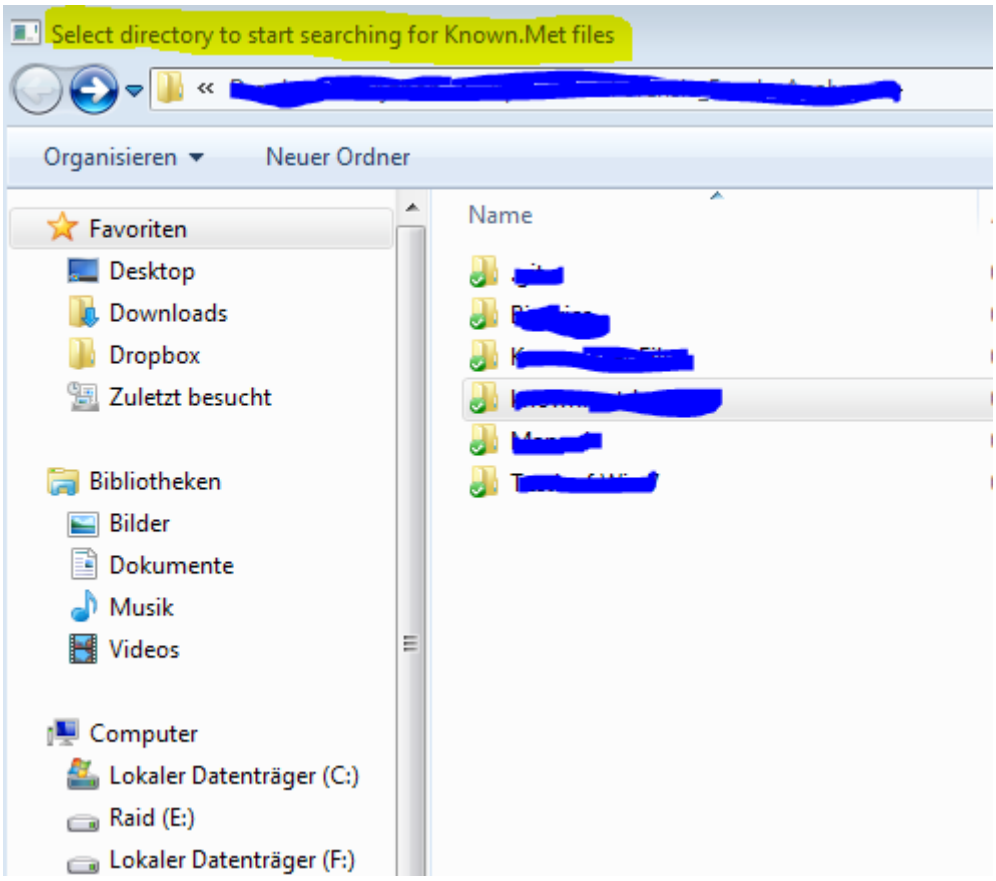
1) Start Forensic Emule Analyzer and select „Parse active Known.Met files““ and „Check results for keywords“ (if you want to check the found filenames against keywords, eg. CP slang). Press „Start“ when ready.



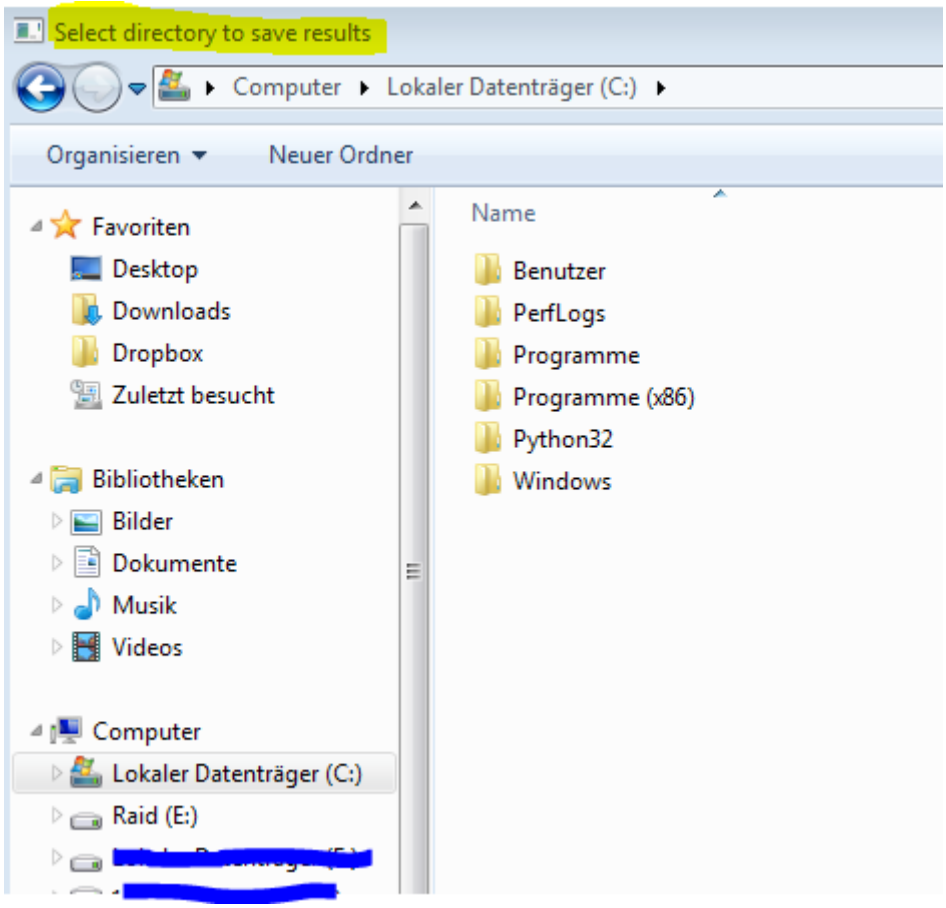
2) Select the file with the keywords. An example keywordsfile ist attached. Read it for more information how to compose a keywordsfile. Use a decent editor like notepad++.



3) Select the directory where to start the search for known.met files.



4) Select the folder for the results.



5) Forensic Emule Analyzer starts to parse the found known.met files and writes the results as TAB separted files to the output folder.