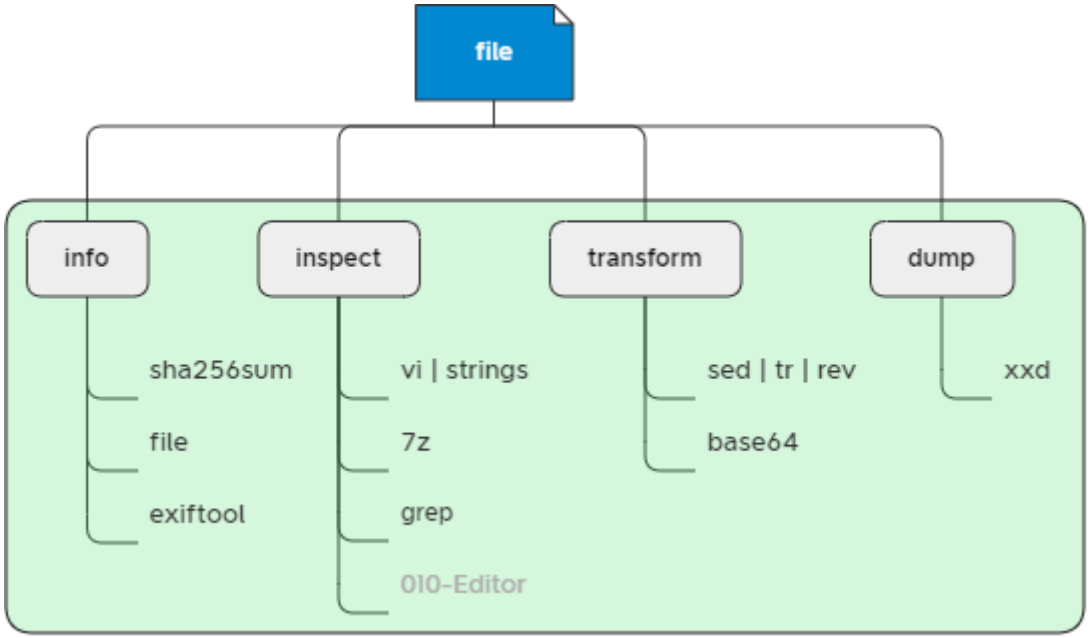
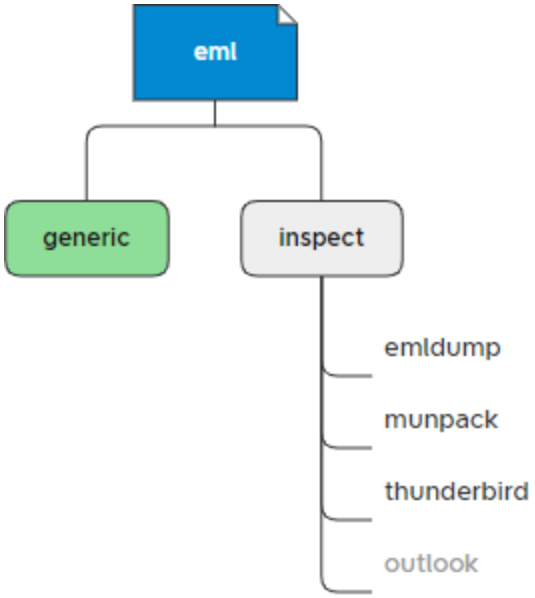
Handling File

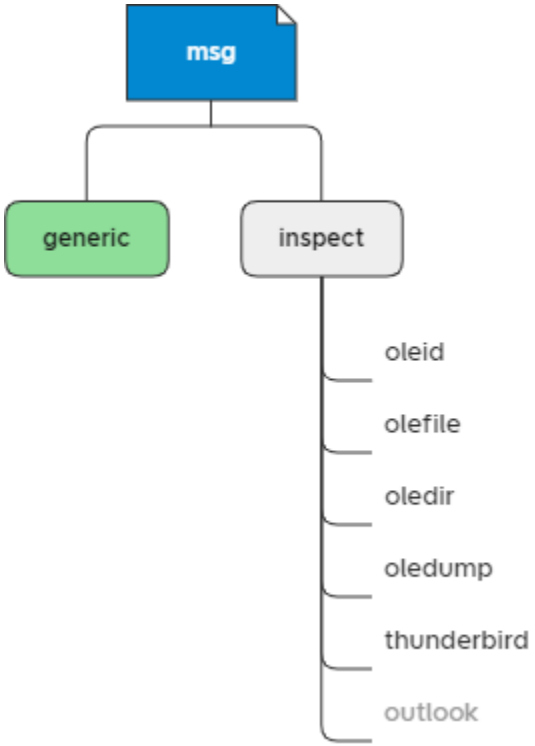


- file extension (when existing) is not reliable
- file signature is based on „magic-bytes"
- gray is Windows only

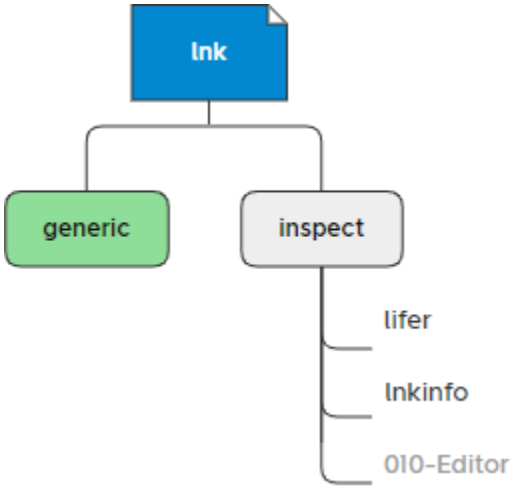
Handling EML File



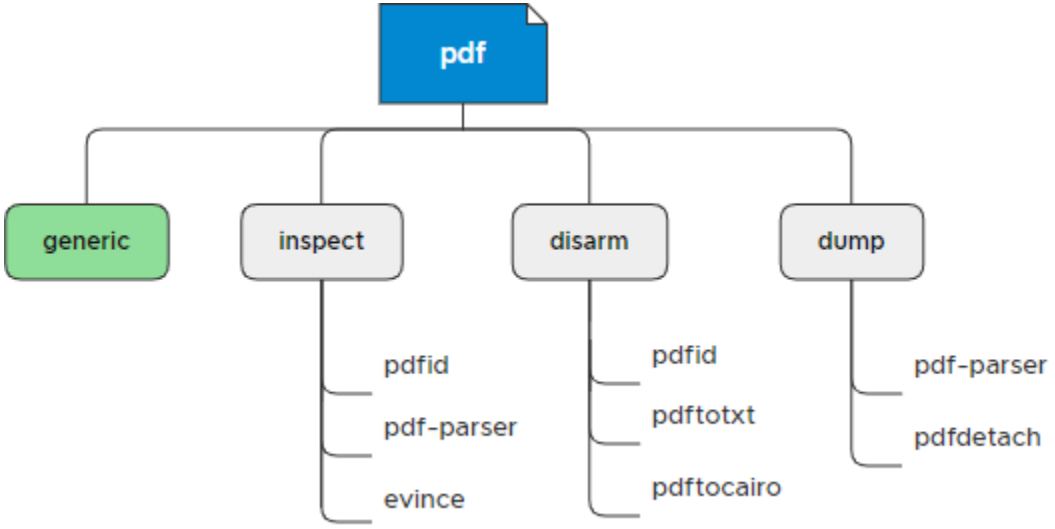
Handling MSG File



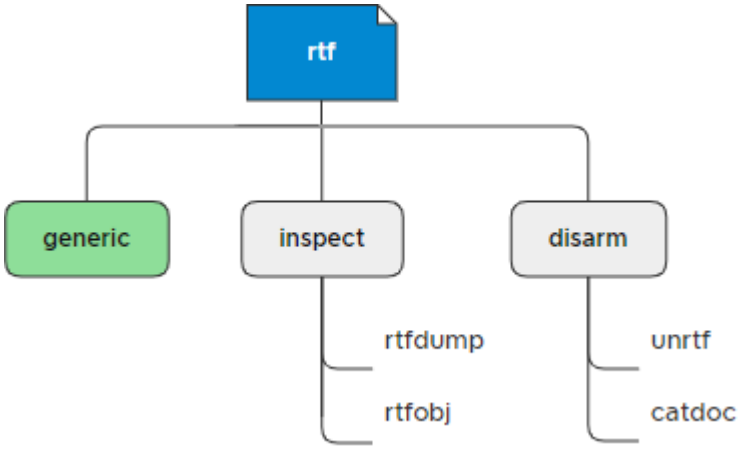
Handling LNK File



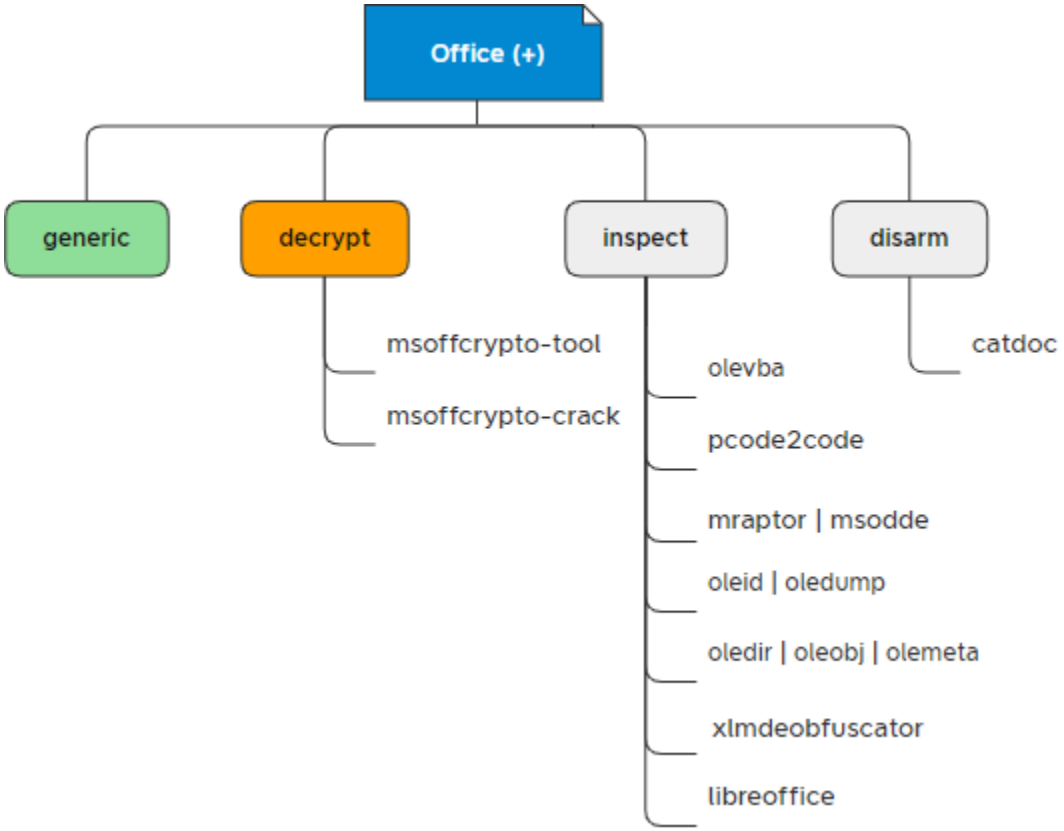
Handling PDF File



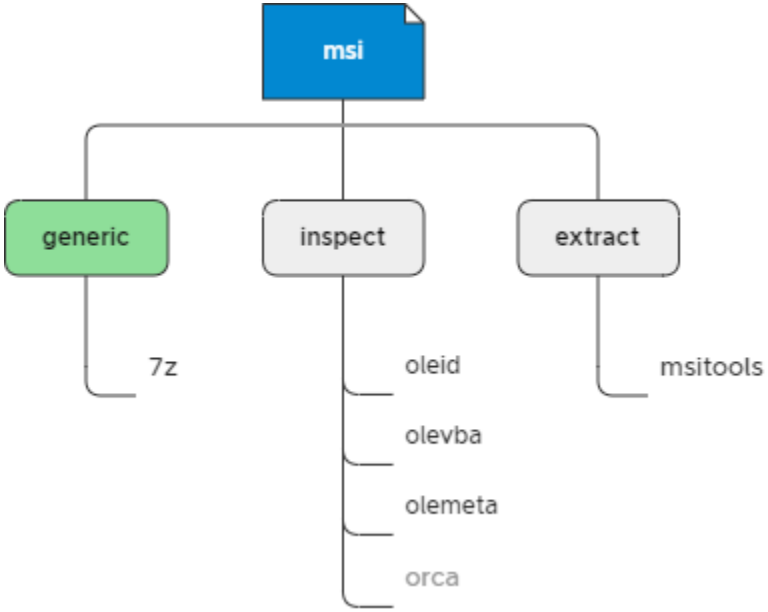
Handling RTF File



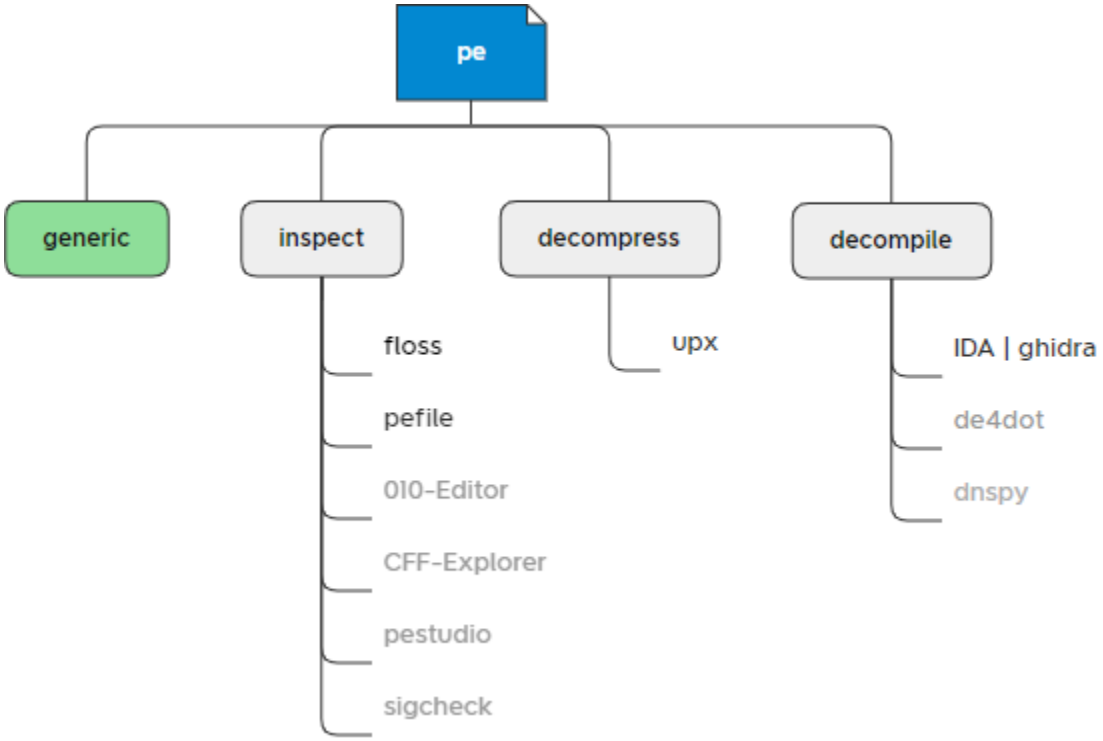
Handling Office File



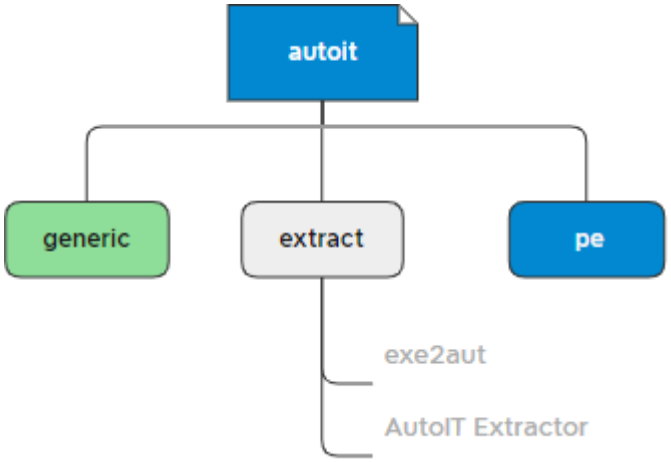
Handling MSI File



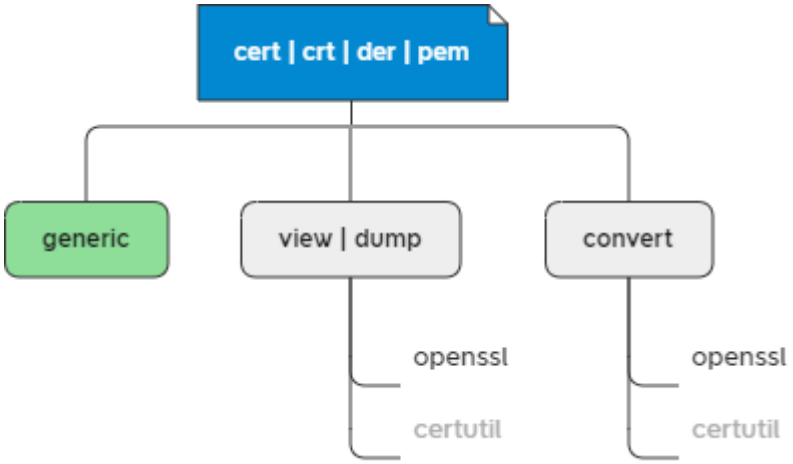
Handling Portable Executable File



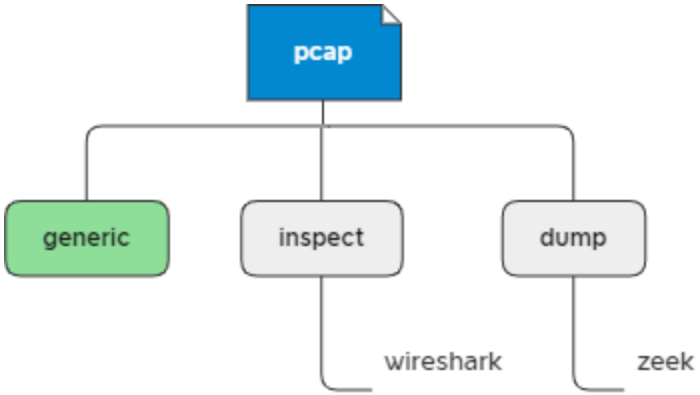
Handling AutoIt Executable File



Handling Certificate File



Handling PCAP File



Links

Oletools	https://github.com/decalage2/oletools
Didier Stevens Tools	https://blog.didierstevens.com/didier-stevens-suite/
Unrtf	http://manpages.ubuntu.com/manpages/bionic/man1/unrtf.1.html
Catdoc	http://www.wagner.pp.ru/~vitus/software/catdoc/
Floss	https://github.com/mandiant/flare-floss
Mraptor	https://github.com/decalage2/oletools/wiki/mraptor
Xlmmacrodeobfuscator	https://github.com/DissectMalware/XLMMacroDeobfuscator
Orca	https://docs.microsoft.com/en-us/windows/win32/msi/orca-exe
pdfdetacher	https://poppler.freedesktop.org/
AutoIT Extractor	https://gitlab.com/x0r19x91/autoit-extractor
Uncompyle2	https://github.com/wibiti/uncompyle2
pcode2code	https://github.com/Big5-sec/pcode2code

Links

lifer	https://github.com/Paul-Tew/lifer
scrdec	http://df2anarchy.free.fr/htana/hack/hack4.html
de4dot	https://github.com/de4dot/de4dot
Hanword document convertor	https://www.microsoft.com/en-us/download/details.aspx?id=36772
zeek	https://zeek.org