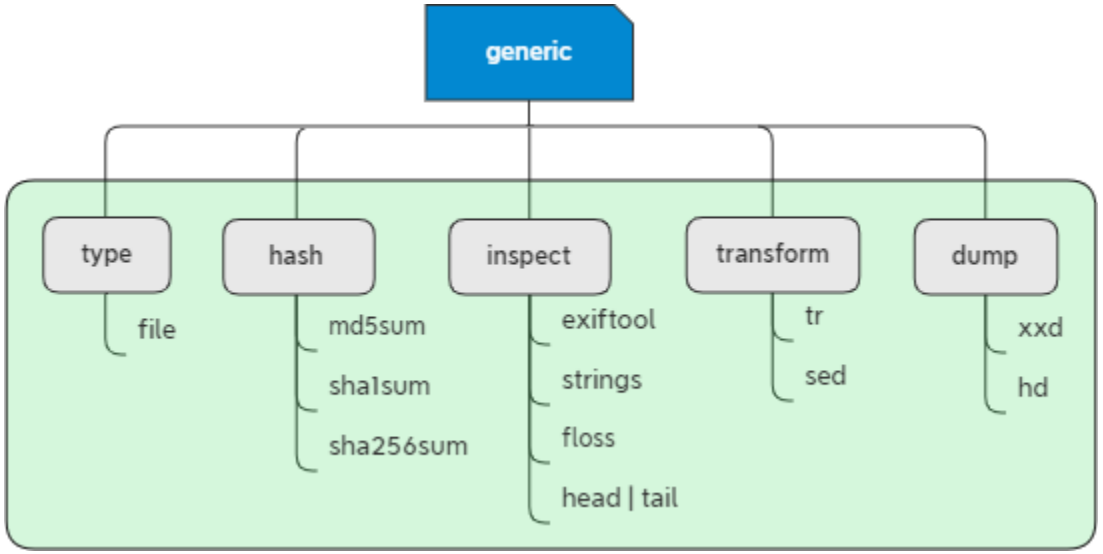
Malware Analysis Fundamentals - Files | Tools

August 21, 2020

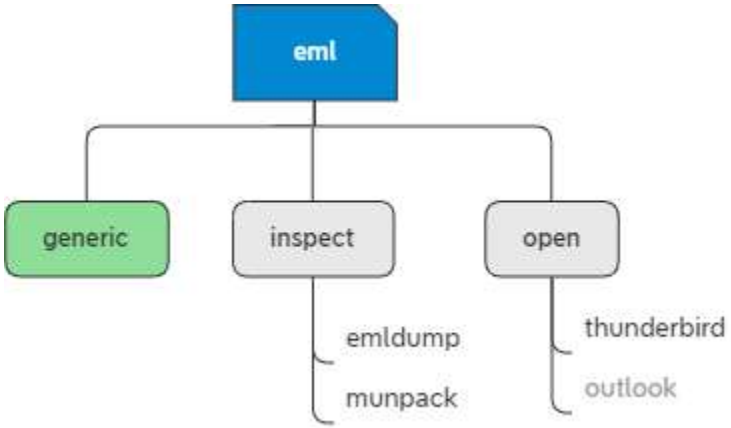
Marc Ochsenmeier
@ochsenmeier
www.winitor.com

Handling generic |unknown File

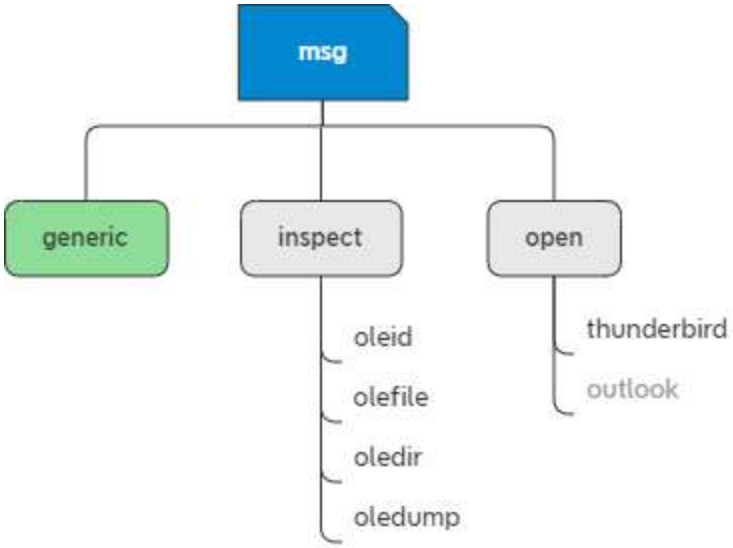


(In this document, grayed items are tools running on Windows)

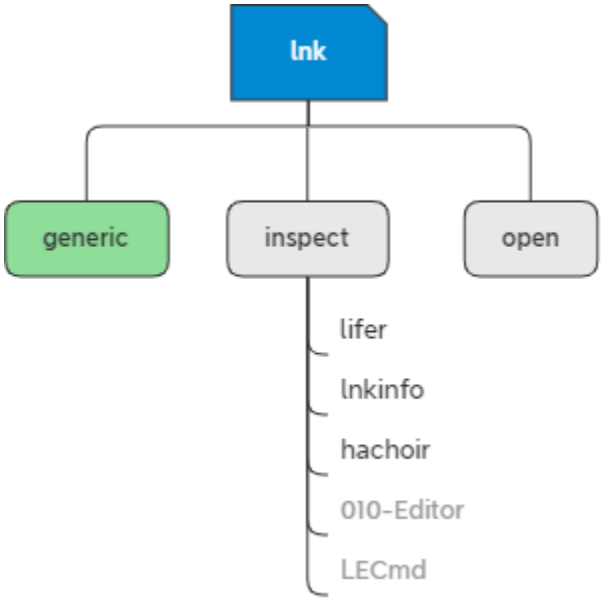
Handling EML File



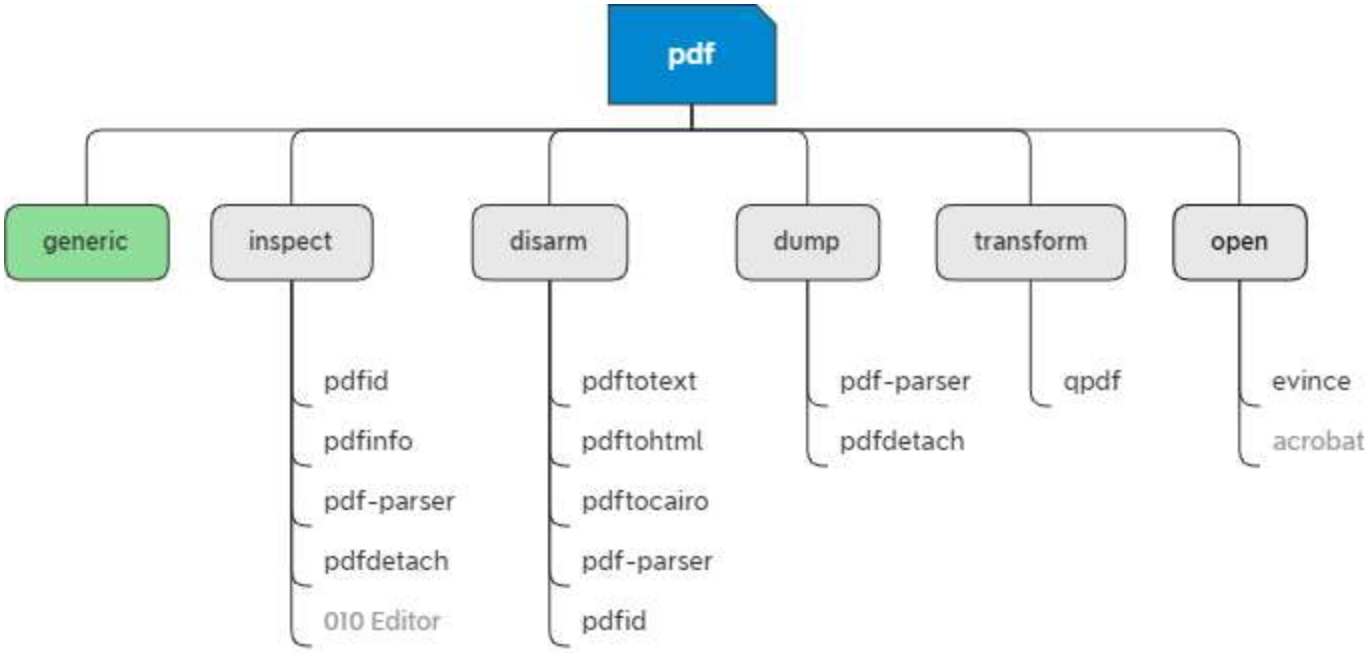
Handling MSG File



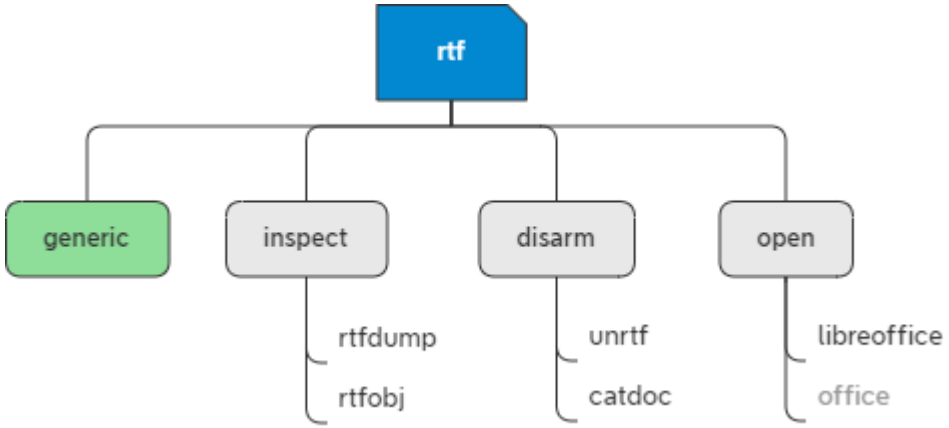
Handling LNK File



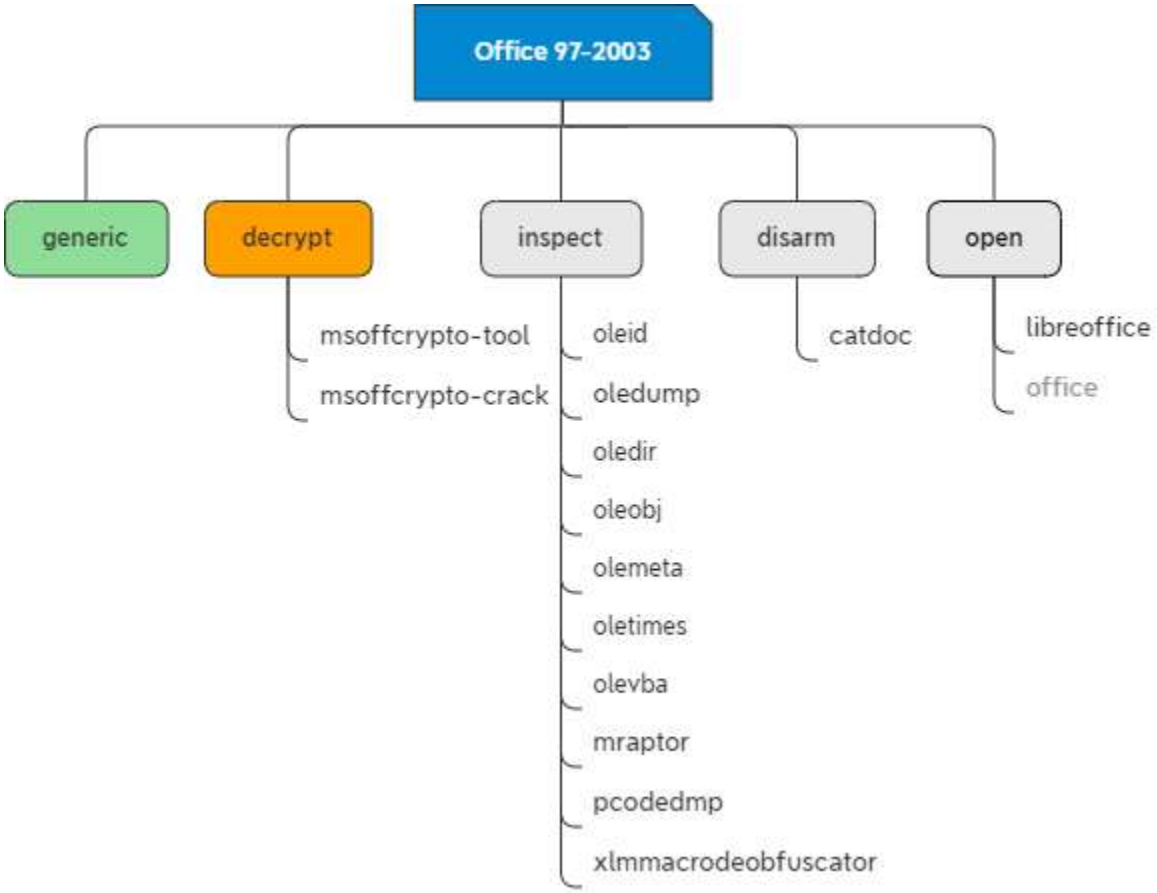
Handling PDF file



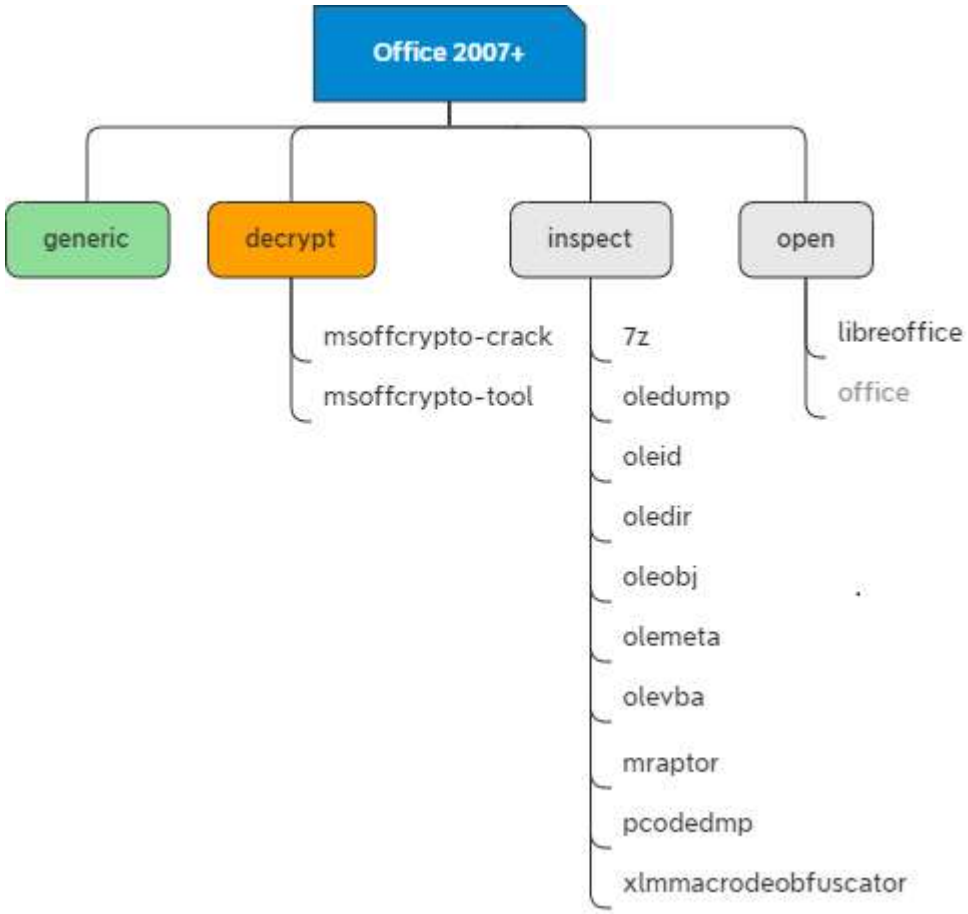
Handling RTF File



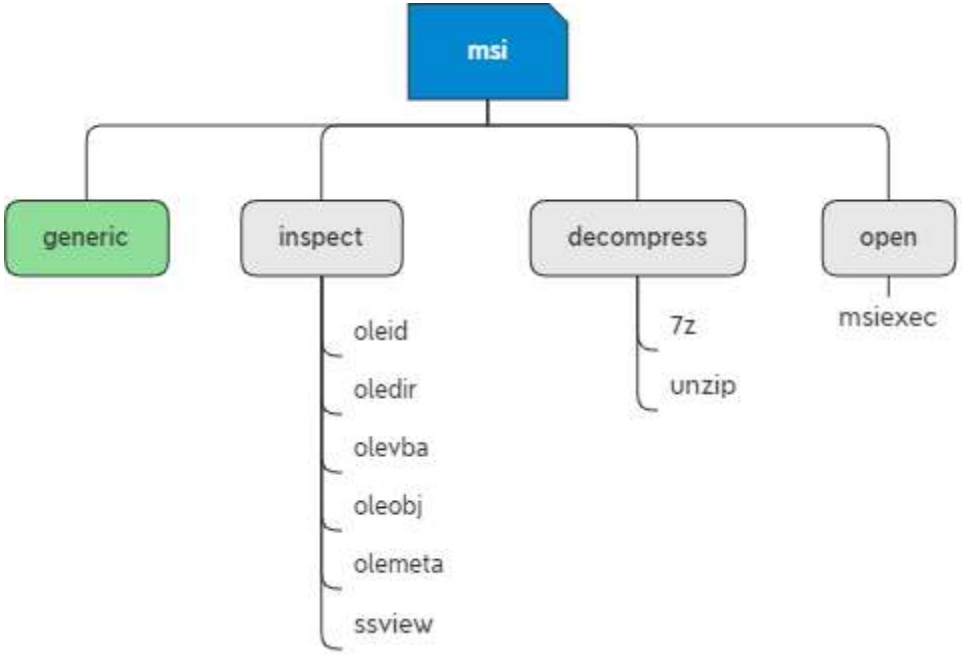
Handling Office 97-2003 File



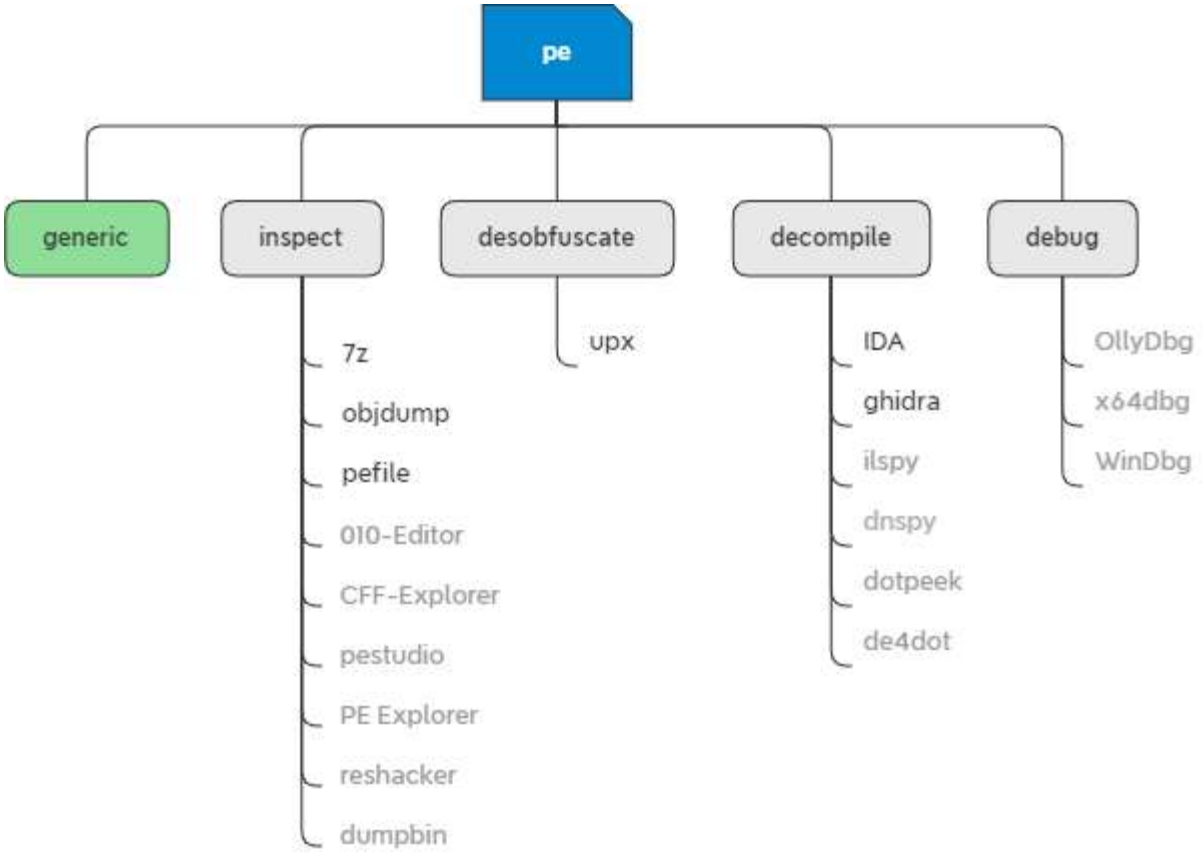
Handling Office 2007+ File



Handling MSI File

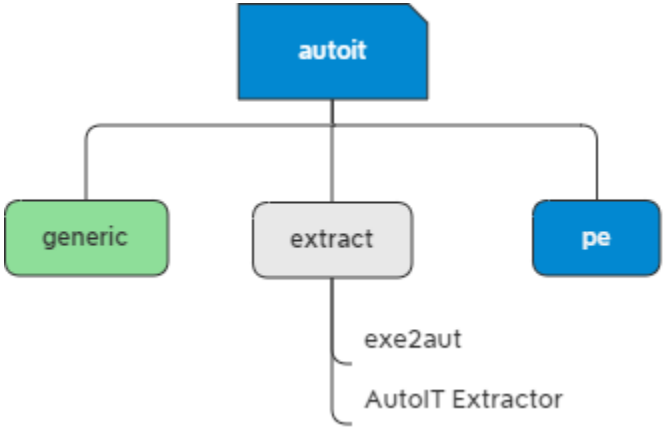


Handling Executable File

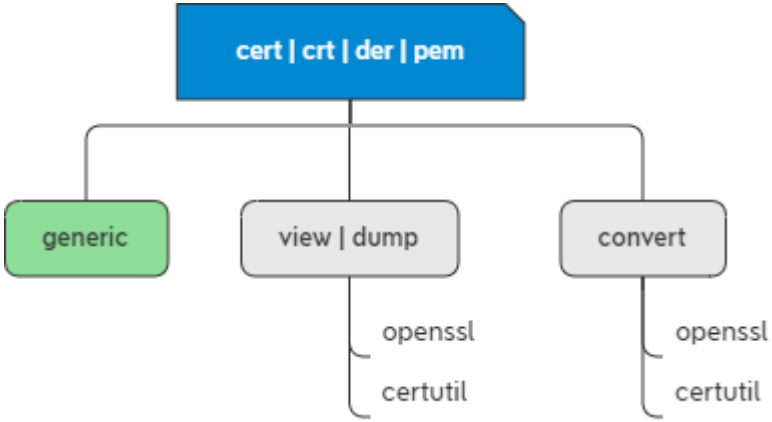


.exe, .dll, .scr, .cpl, .sys, .mui, .ocx, .acm, ...

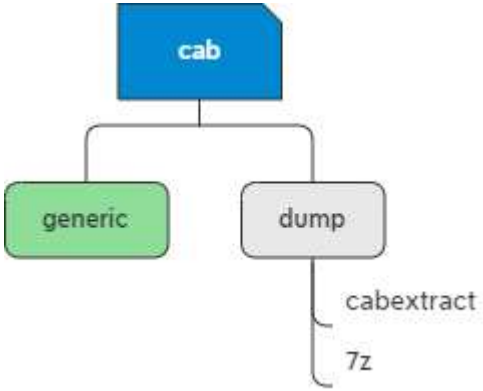
Handling AutoIt Executable File



Handling Certificate File



Handling Cab File



Handling Office File

	rtf	doc	dot	docx	docm	dotm	xls	xlsx	xlsb	xlsm	ppt	pptm	ppsm	pub	slk	msg
unzip	-	-	-	x	-	-	-	x	x	x	-	-	-			-
exiftool	x	x		x			x	x	-	x						x
file	x	x	x	x	x	x	x	x	-		x	x	x			-
libre-office	x	x	~	x			x									-
ms-offcrypto-tool	-	~		x												-
msoffcrypto-crack	-	~		x												-
oledir	-	x	x	~	x	x	x	x	-	x	x	x	x	x		x
oledump	-	x	x	~	x	x	x	x	-	x	x	x	x	x		x
oleid	-	x	x	~	x	x	x	x	-	x	x	x	x	x		x
oleobj	-	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
olevba	-	x	x	x	x	x	x	x	x	x	x	x	x	x	x	-
rtfdump	x	-		-			-		-							-
rtfobj	x	-		-			-		-							-
strings	x	x	x	x	x	x	x		x		x	x	x			x
emldump	-	-	-	-	-	-	-	-	-	-	-	-	-			-
floss	x	x	x	x	x	x	x	x	x	x	x	x	x			x
7z	-	-	-	x	-	-	-	-	-	-	-	-	-			-
ssview	-	x	x	-	-	-	-	-	-	-	-	-	-	-	-	x
word pad	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
xlmmacrodeobfuscator	-	-	-	-	-	-	x	x	x	x	-	-	-	-	-	-
unrtf	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
catdoc	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-
mraptor	-	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Handling other File

	msg	eml	tlb	cer	crt	der	pem	cab	a3x	exe	msi	lnk	pyc
unzip	-	-	-	-	-	-	-		-	-	x	-	-
exiftool	-	x	-	-	-	-	-	-	x	x	x	x	
file	x	x	-	-	-	-		x	x	x	x	x	x
strings	x	x	-	-	-	-	-	x	-	x	x	x	-
emldump	-	x	-	-	-	-	-	-	-	-	-	-	-
floss	x	x	-	-	-	-	-	x	x	x	x	x	-
dumpbin	-	-	-	-	-	-	-	-	-	x	-	-	-
objdump	-	-	-	-	-	-	-	-	-	x	-	-	-
certutil	-	-	-	x	x	x	x	-	-	-	-	-	-
openssl	-	-	-	x	x	x	x	-	-	-	-	-	-
7z	-	-	-	-	-	-	-	x	-	x	x	-	-
upx	-	-	-	-	-	-	-	-	x	x	-	-	-
cabextract	-	-	-	-	-	-	-	x	-	-	-	-	-
ssview	-	-	-	-	-	-	-	-	-	-	x	-	-
Exe2aut	-	-	-	-	-	-	-	-	-	x	-	-	-
AutoIT-Extractor	-	-	-	-	-	-	-	-	-	x	-	-	-
010-editor										x		x	-
LECmd	-	-	-	-	-	-	-	-	-	-	-	x	-
thunderbird	x	x	-	-	-	-	-	-	-	-	-	-	-
munpack	?	x	-	-	-	-	-	-	-	-	-	-	-
lifer	-	-	-	-	-	-	-	-	-	-	-	x	-
lnkinfo	-	-	-	-	-	-	-	-	-	-	-	x	-
uncompyle6	-	-	-	-	-	-	-	-	-	-	-	-	x

	pdf
exiftool	x
file	x
strings	x
floss	x
pdfid	x
pdf-parser	x
pdftotext	x
pdftocairo	x
pdftohtml	x
pdfdetach	x
evince	x
qpdf	x

Links

- oletools
  https://github.com/decalage2/oletools
- Didier Stevens
  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/
- mraptor
  https://github.com/decalage2/oletools/wiki/mraptor
- xlmmacrodeobfuscator
  https://github.com/DissectMalware/XLMMacroDeobfuscator
- pcodedmp.py - A VBA p-code disassembler
  https://github.com/bontchev/pcodedmp
- Analyzing Malicious Documents Cheat Sheet
  https://zeltser.com/media/docs/analyzing-malicious-document-files.pdf

Links

- pdfdetacher
  https://poppler.freedesktop.org/
- qpdf
  https://sourceforge.net/projects/qpdf/
- AutoIT Extractor
  https://gitlab.com/x0r19x91/autoit-extractor
- uncompyle2
  https://github.com/wibiti/uncompyle2
- LECmd
  https://f001.backblazeb2.com/file/EricZimmermanTools/LECmd.zip
- Lifer
  https://github.com/Paul-Tew/lifer