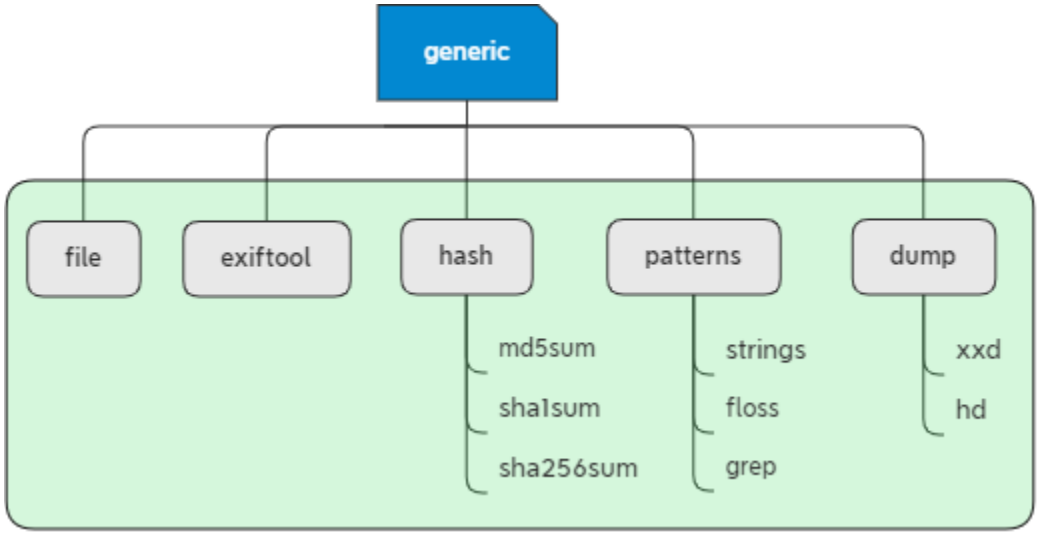
Malware Analysis Fundamentals - Files | Tools

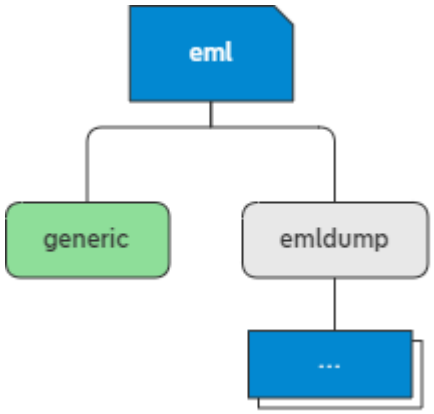
April 02, 2020

Marc Ochsenmeier
@ochsenmeier
www.winitor.com

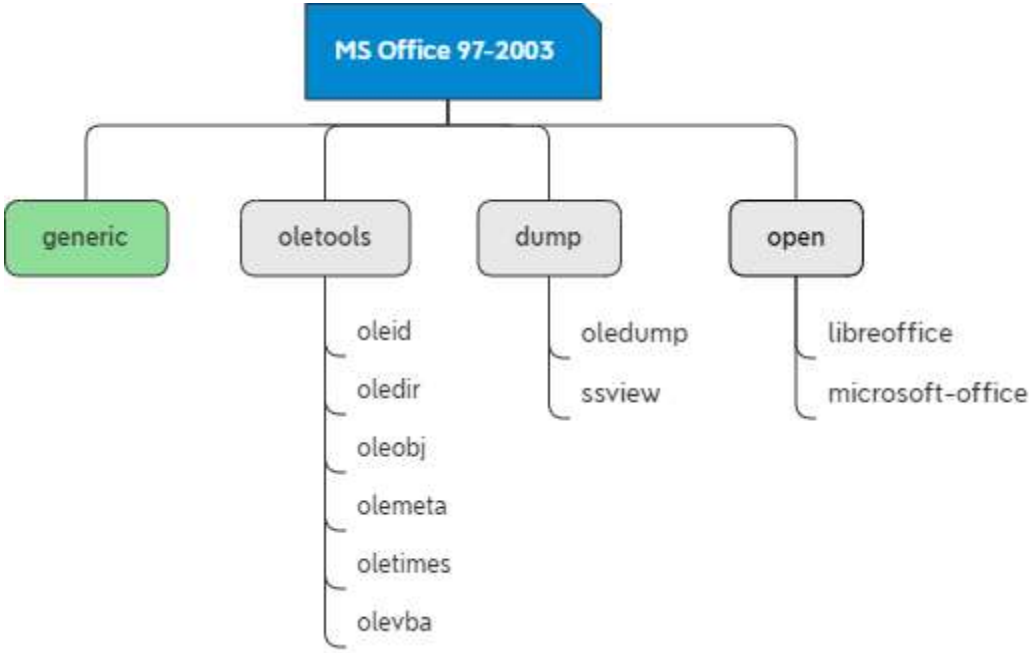
Handling an unknown | generic File



Handling an email File

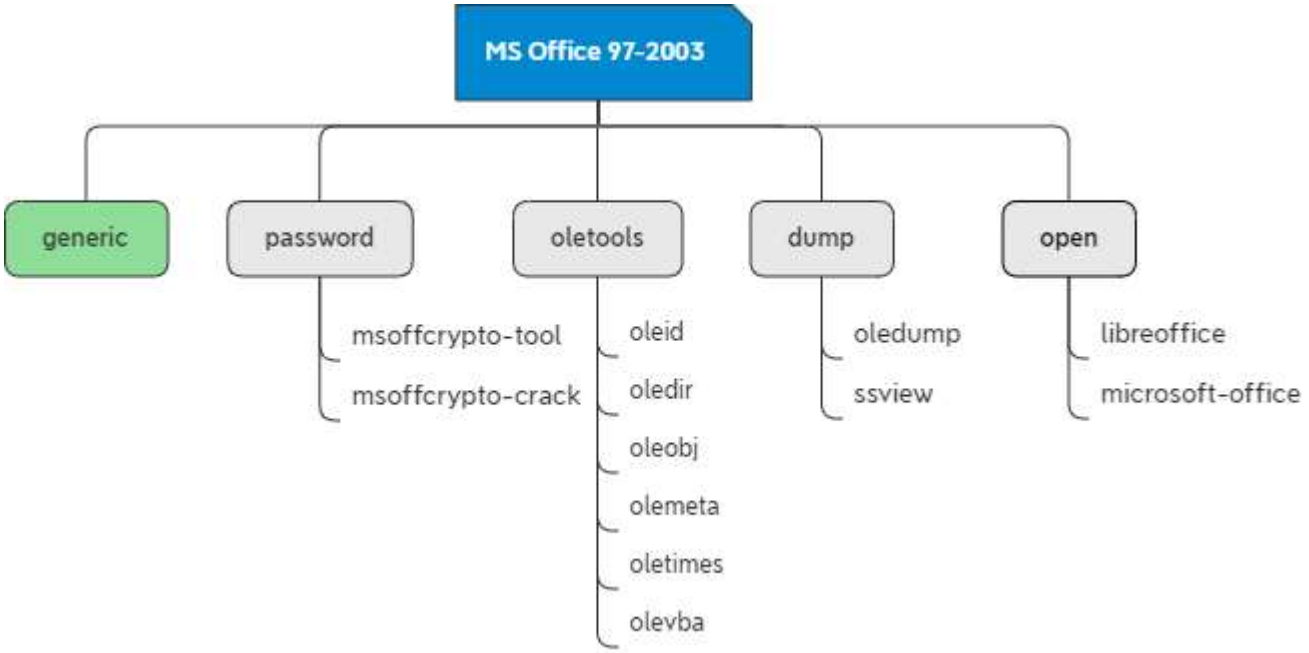


Handling a MS Office 97-2003 File



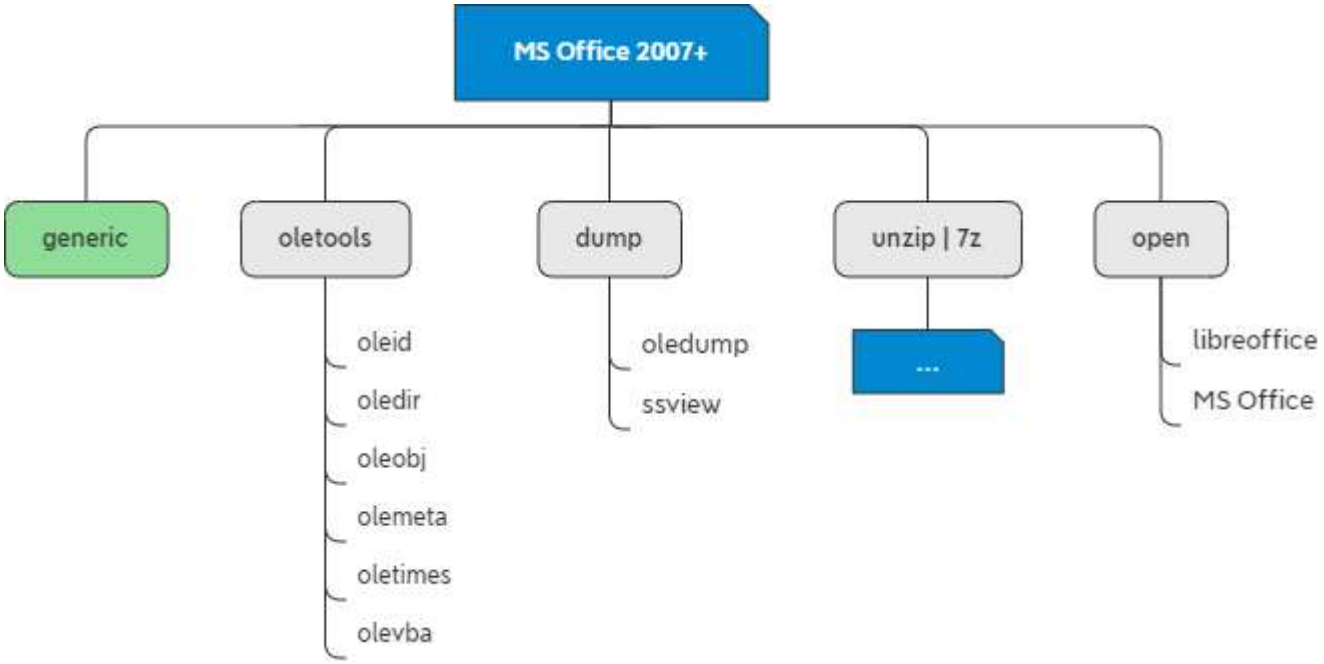
applies to following files: doc, xls, ppt

Handling a protected MS Office 97-2003 File



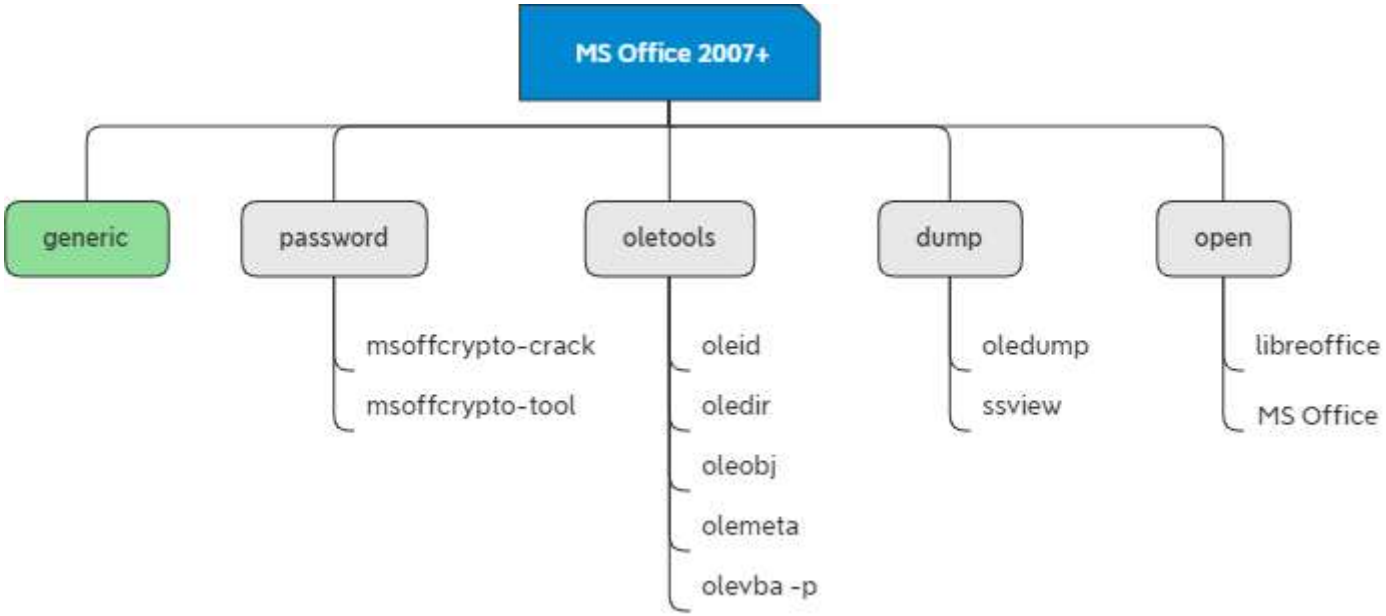
applies to following files: doc, xls, ppt

Handling a MS Office 2007+ File



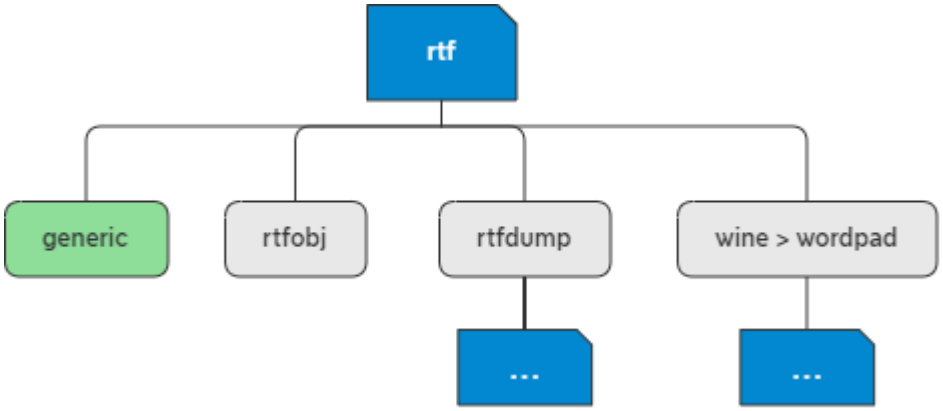
applies to following files: docx, xlsx, xlsb, xlsm, pptx

Handling a protected MS Office 2007+ File

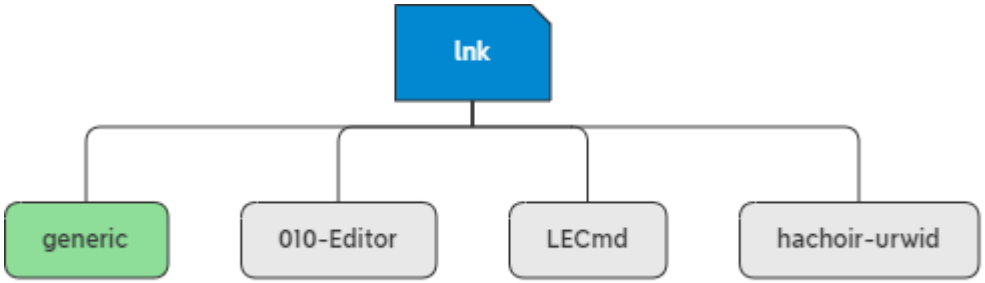


applies to following files: docx, xlsx, xlsb, xlsm, pptx

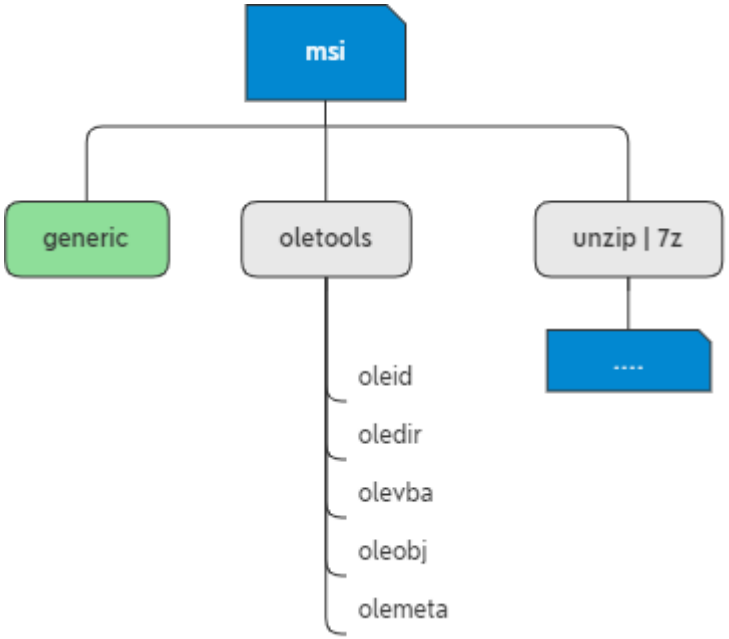
Handling an RTF File



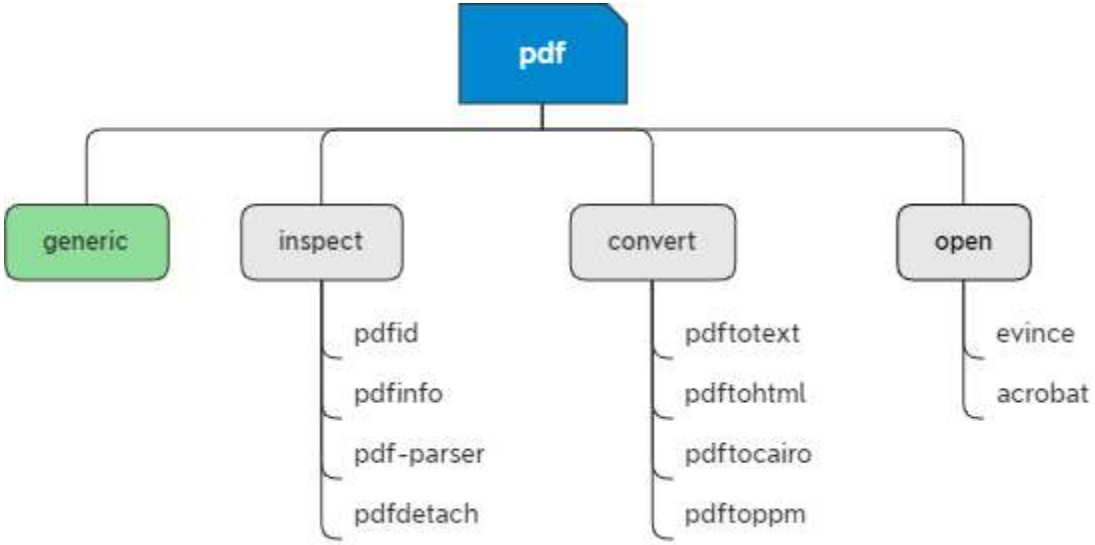
Handling an LNK File



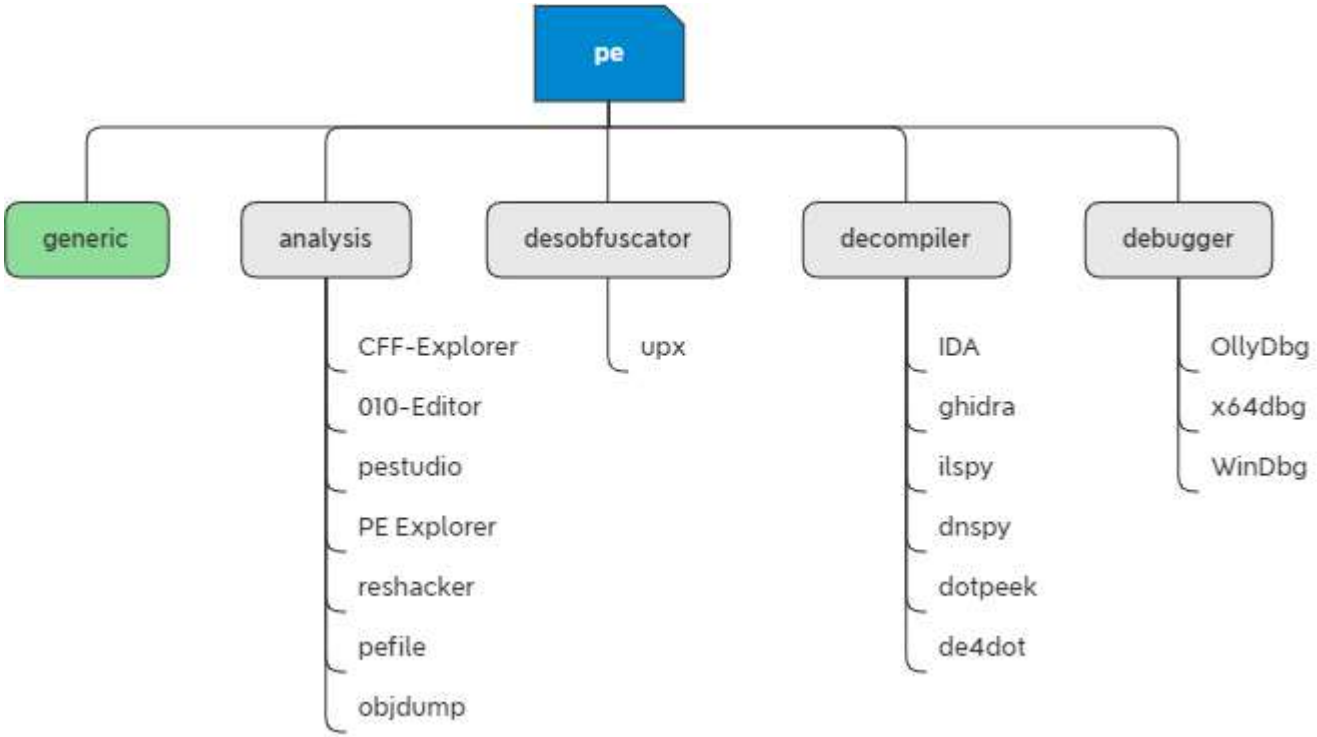
Handling an MSI File



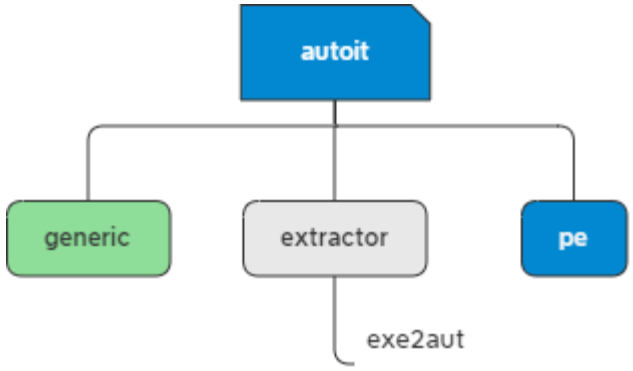
Handling a PDF file



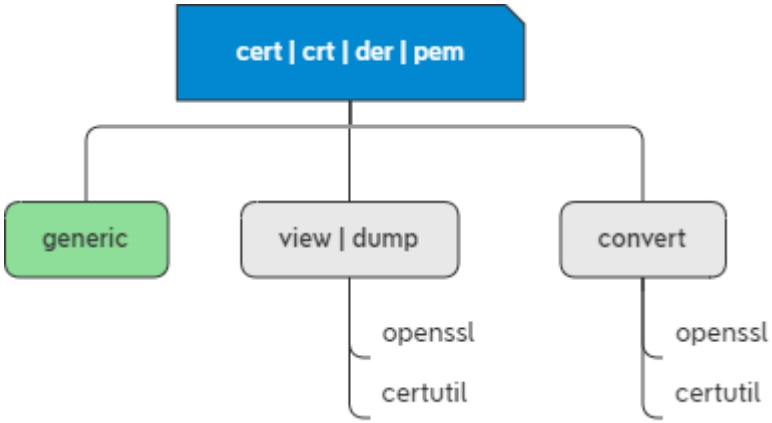
Handling an Executable File



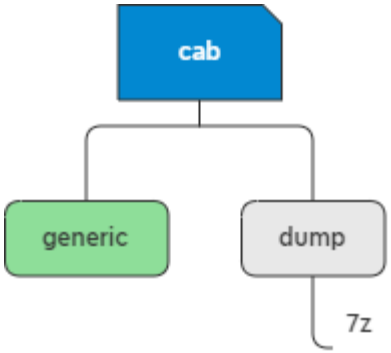
Handling an AutoIt Executable File



Handling a Certificate File



Handling a cab File



Handling Microsoft Office Files

	rtf	doc	dot	docx	docm	dotm	xls	xlsx	xlsb	xlsm	ppt	pptm	ppsm	pub	slk
unzip	-	-	-	x	-	-	-	x	x	x	-	-	-		
exiftool	x	x		x			x	x	-	x					
file	x	x	x	x	x	x	x	x	-		x	x	x		
libre-office	-	x	~	x			x								
ms-offcrypto-tool	-	~		x											
msoffcrypto-crack	-	~		x											
oledir	-	X	x	~	x	x	x	x	-	x	x	x	x	x	
oledump	-	x	x	~	x	x	x	x	-	x	x	x	x	x	
oleid	-	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
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		
emldump	-	-	-	-	-	-	-	-	-	-	-	-	-		
floss	x	x	x	x	x	x	x	x	x	x	x	x	x		
7z	-	-	-	x	-	-	-	-	-	-	-	-	-		
ssview	-	x	x	-	-	-	-	-	-	-	-	-	-	-	-

Handling miscellaneous Files

	msg	eml	tlb	cer	crt	der	pem	cab	a3x	exe	pdf	msi
unzip	-	-	-	-	-	-	-		-	-	-	x
exiftool	-	x	-	-	-	-	-	-	x	x	x	
file	x	x	-	-	-	-		x	x	x	x	
strings	x	x	-	-	-	-	-	x	-	x	x	
emldump	-	x	-	-	-	-	-	-	-	-	-	
floss	x	x	-	-	-	-	-	x	x	x	x	
certutil	-	-	-	x	x	x	X	-	-	-	-	-
openssl	-	-	-	x	x	x	x	-	-	-	-	-
7z	-	-	-	-	-	-	-	x	-	-	-	x
upx	-	-	-	-	-	-	-	-	x	x	-	-
pdfid	-	-	-	-	-	-	-	-	-	-	x	-
pdf-parser	-	-	-	-	-	-	-	-	-	-	x	-
pdftotext	-	-	-	-	-	-	-	-	-	-	x	-
pdftocairo	-	-	-	-	-	-	-	-	-	-	x	-
pdftohtml	-	-	-	-	-	-	-	-	-	-	x	-
evince	-	-	-	-	-	-	-	-	-	-	x	-

More Information

- python-oletools
  https://github.com/decalage2/oletools
- Didier Stevens
  https://blog.didierstevens.com/didier-stevens-suite/
- Analyzing Malicious Documents Cheat Sheet
  https://zeltser.com/media/docs/analyzing-malicious-document-files.pdf