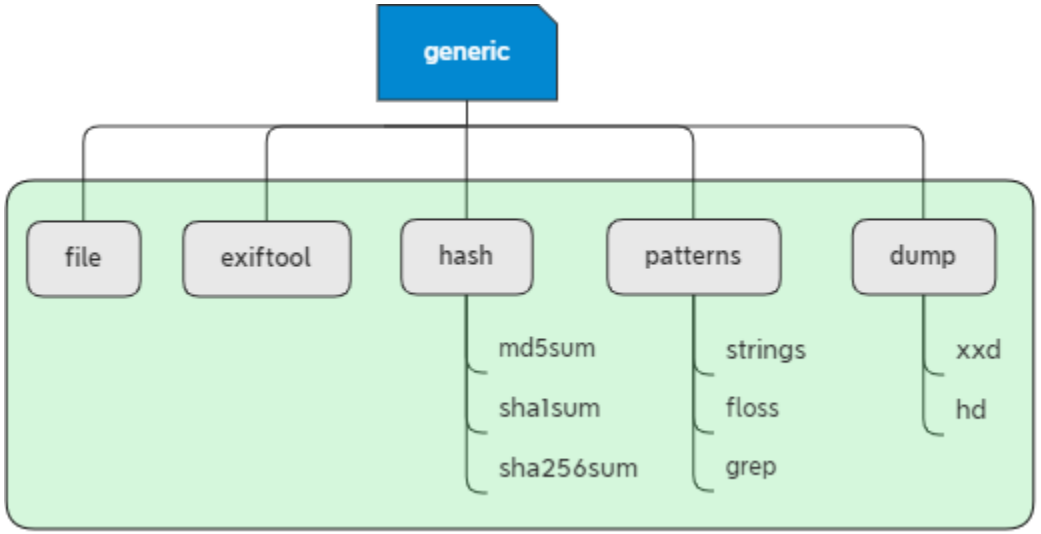
Malware Analysis Fundamentals - Files | Tools

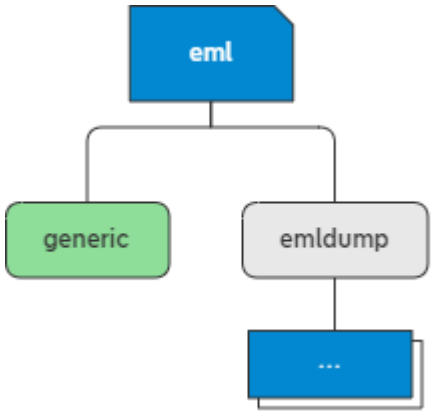
March 27, 2020

Marc Ochsenmeier
@ochsenmeier
www.winitor.com

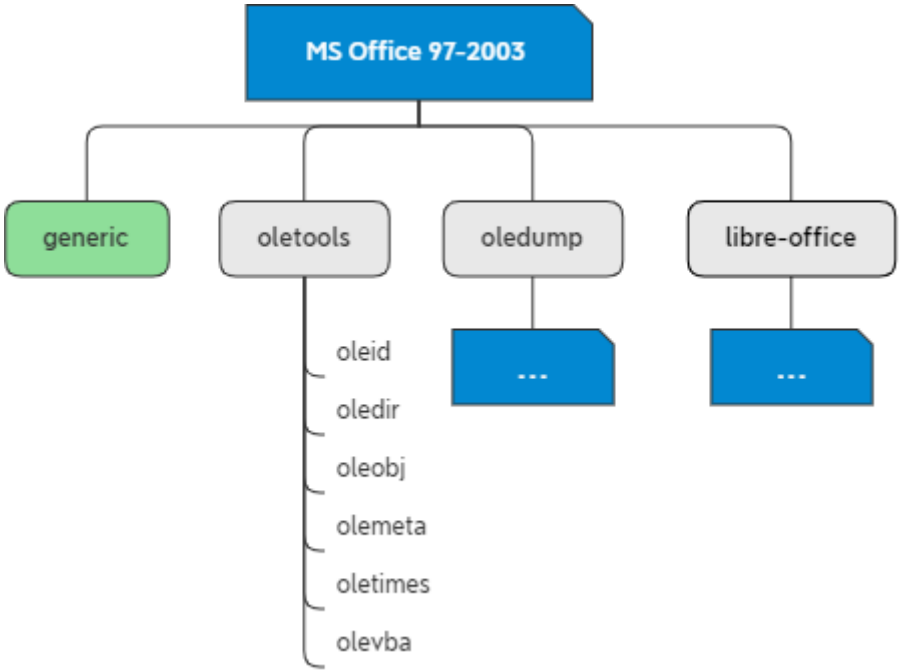
Handling an unknown | generic File



Handling an email File

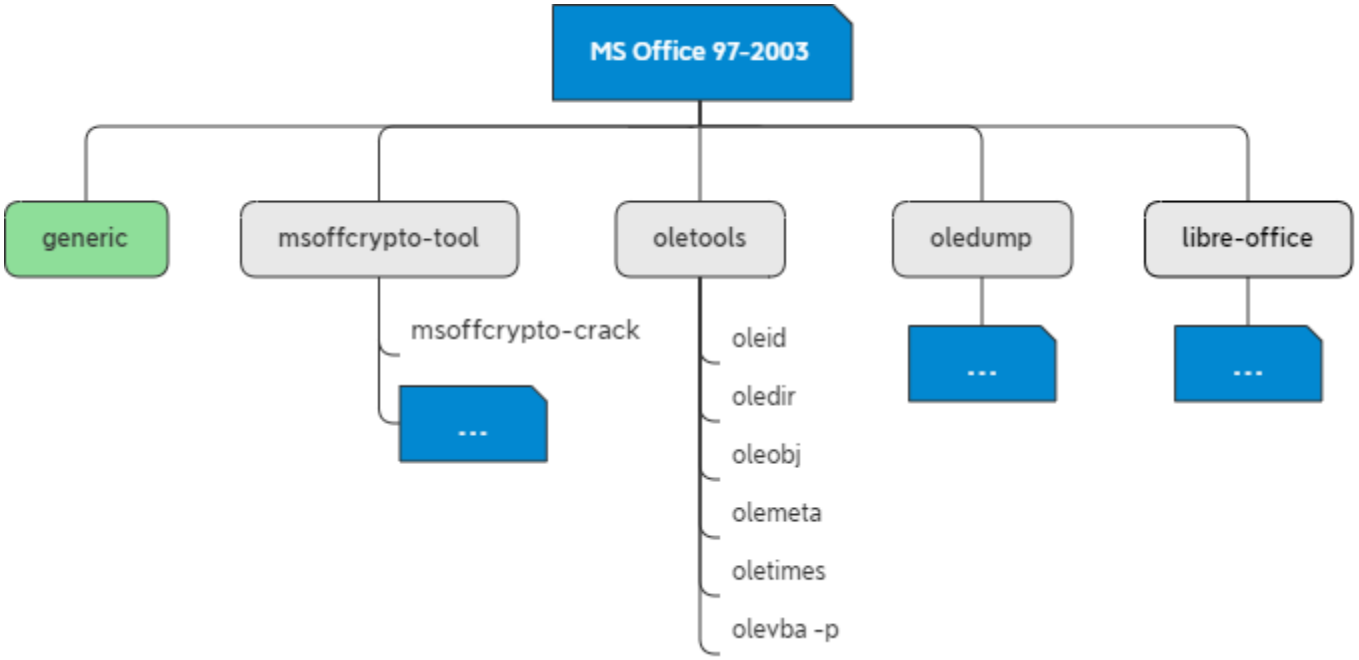


Handling a MS Office 97-2003 File



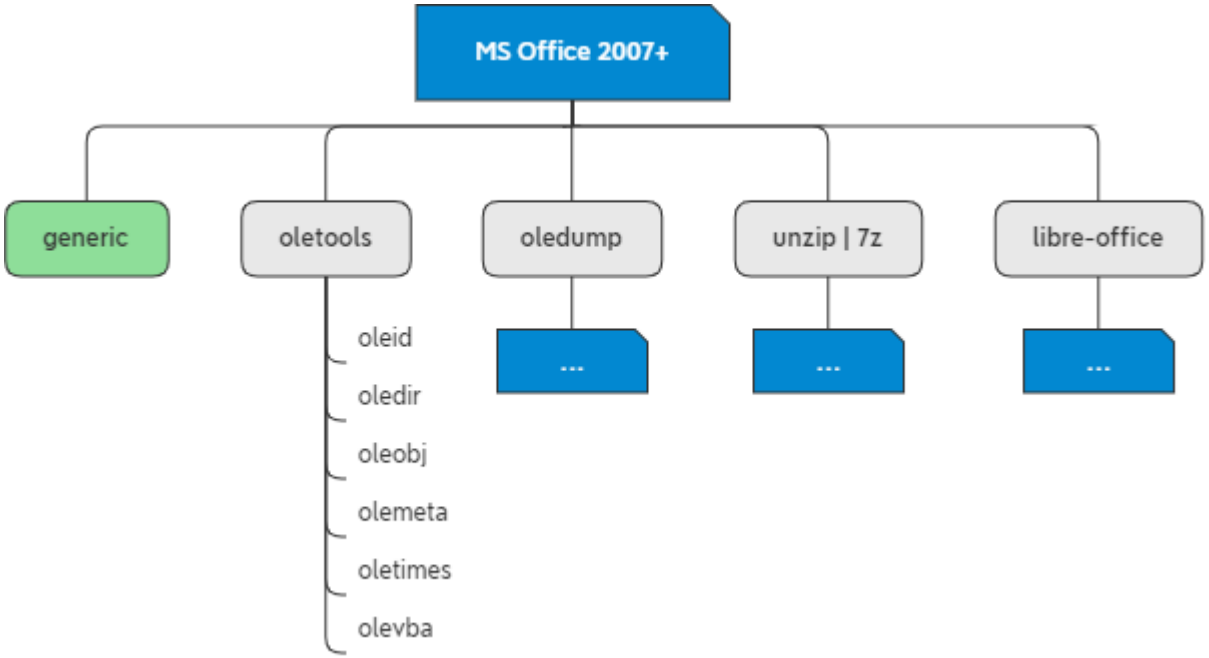
applies to following files: doc, xls, ppt, msg

Handling a protected MS Office 97-2003 File



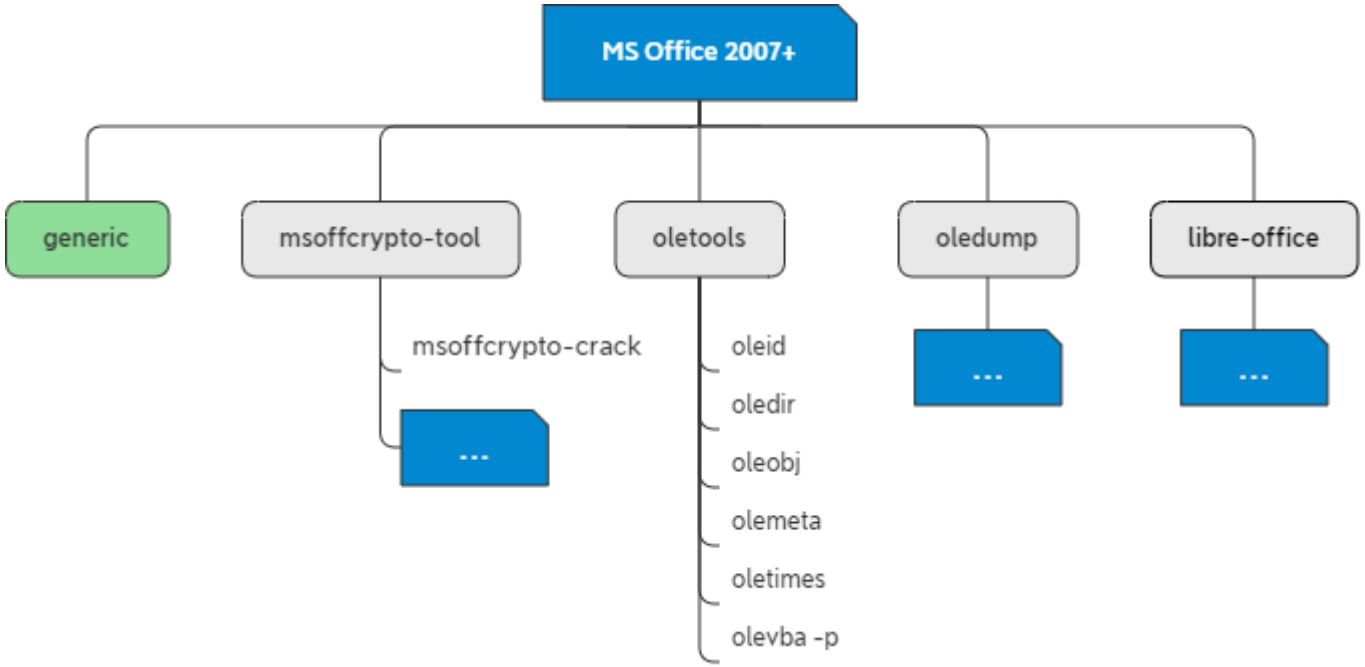
applies to following files: doc, xls, ppt, msg

Handling a MS Office 2007+ File



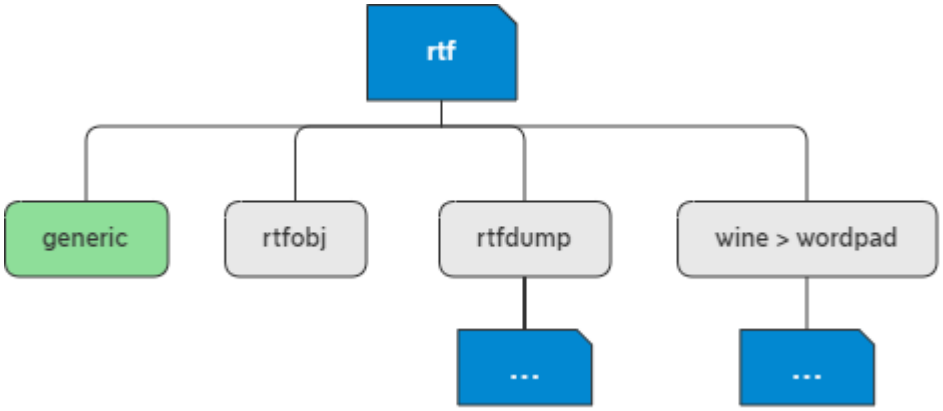
applies to following files: docx, xlsx, xlsb, xlsm, pptx

Handling a protected MS Office 2007+ File

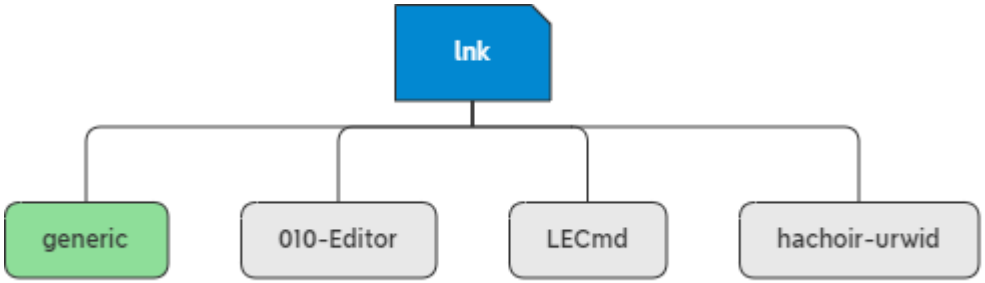


applies to following files: docx, xlsx, xlsb, xlsm, pptx

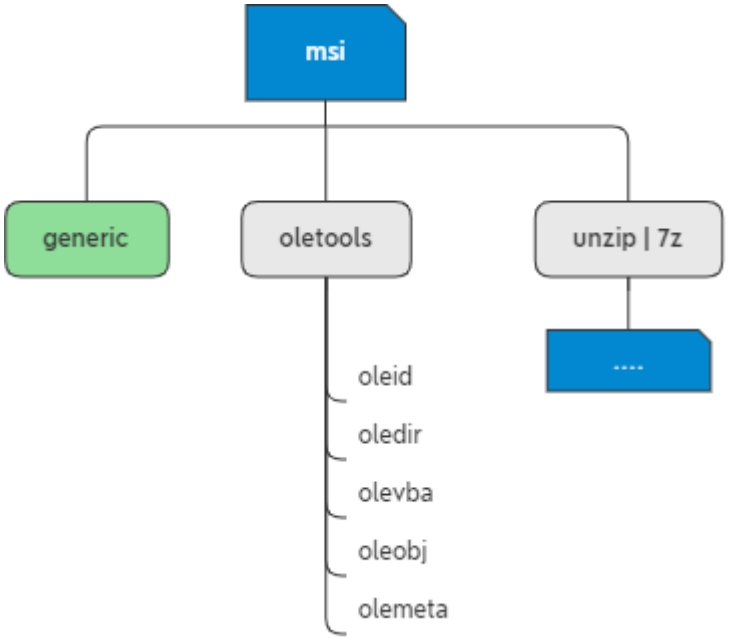
Handling an RTF File



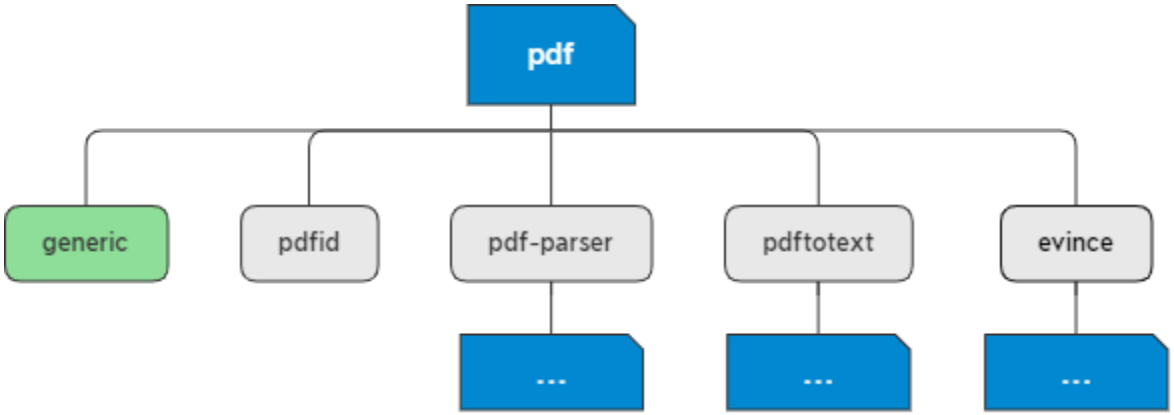
Handling an LNK File



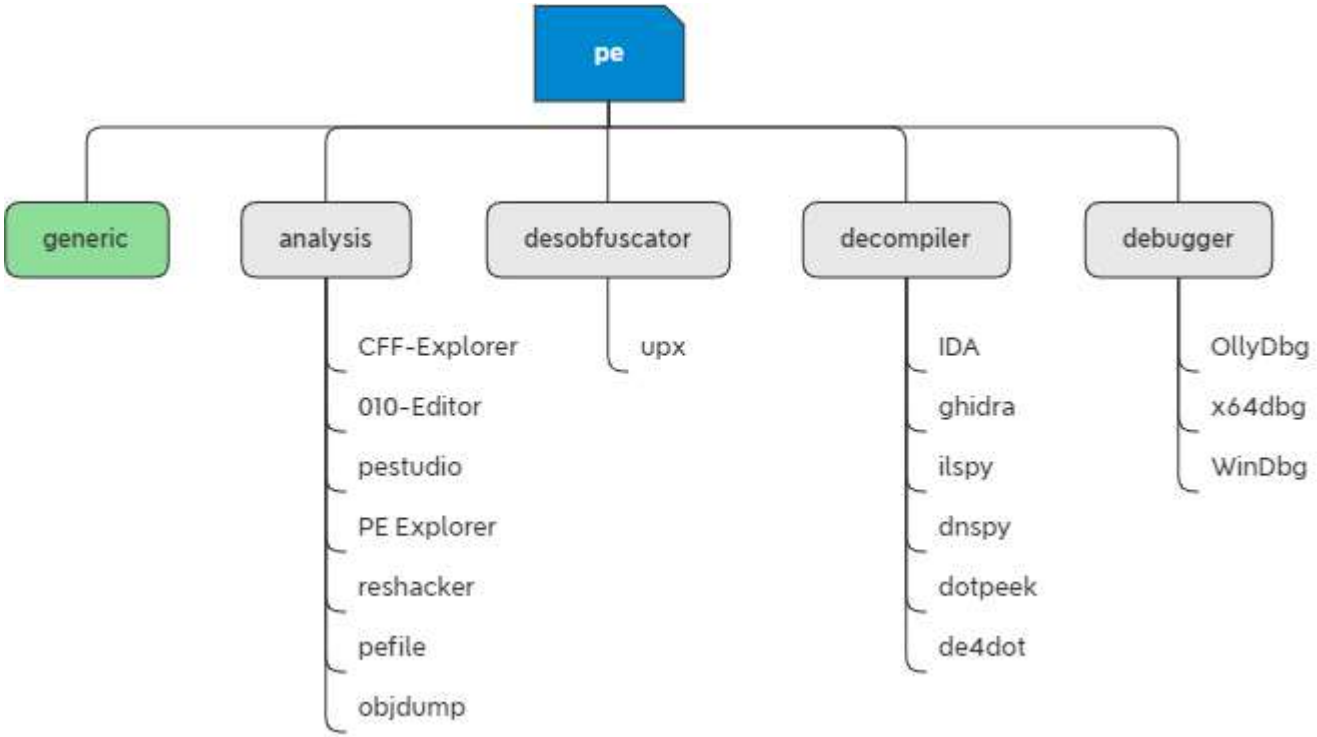
Handling an MSI File



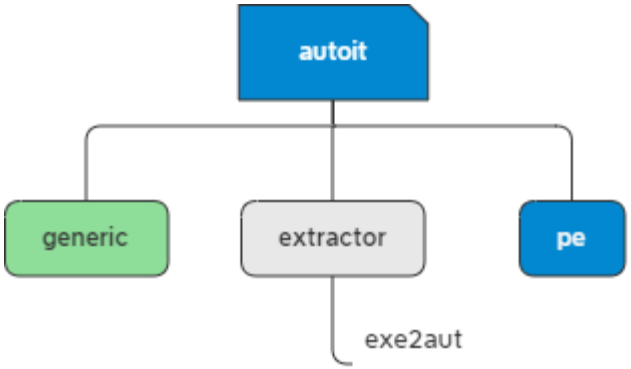
Handling a PDF file



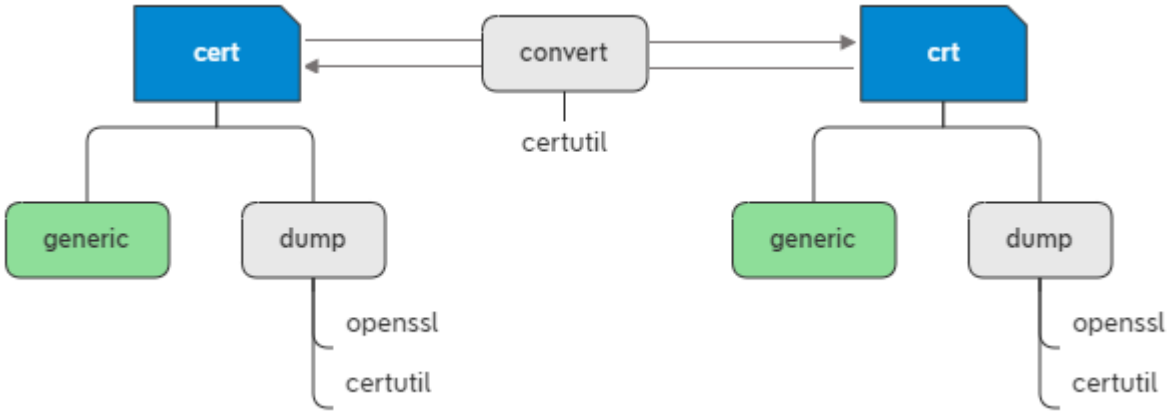
Handling an Executable File



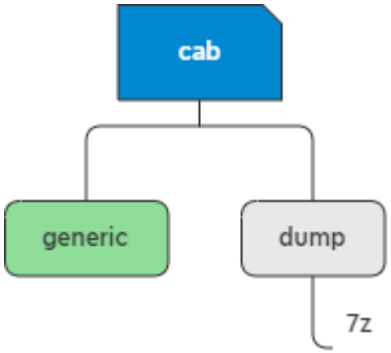
Handling an AutoIt Executable File



Handling a Certificate File



Handling a cab File



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