www.winitor.com - pestudio 9.08 features

This table shows the features of **pestudio** and **pestudio professional**

Feature	pestudio	pestudio-pro
detect file signature	x	x
detect hardcoded URL and IP addresses	x	x
detect dos-stub message	x	x
detect debug information	x	x
detect exceptions and TLS callback function	x	x
detect functions	x	x
detect blacklist strings	x	x
compute entropy	x	x
compute Imphash	x	x
compute file-ratio	x	x
show first bytes of entry-point, resources and overlay	x	x
blacklist section name	x	x
indicate self-modifying sections	x	x
show **Virustotal** score	x	x
dump resources (ico, version, strings tables, ...)	x	x
dump overlay	x	x
detect imports by ordinals	x	x
detect deprecated, blacklist and undocumented imports	x	x
detect duplicated exports	x	x
detect whitelist strings	x	x
detect file(s) embedded in overlay	x	x
blacklist signature of resource	x	x
query imports and exports functions @ MSDN	x	x
compute hash of file with and without overlay	x	x
retrieve date-time-stamps from directories	x	x
query Google on resources Hash	x	x
search **Virustotal** for Impash (*)	x	x
show hints and their friendly names	x	x
URL links to google on hash, pdb	x	x
show exceptions table	x	x
show relocations table	x	x
show functions groups	x	x
configure the tool using context menus	partial	x
URL links to **MITRE**	-	x
blacklist file signatures selected in signatures.xml	-	x

Feature	pestudio	pestudio-pro
dump PKCS7 of certificate	-	x
delete overlay	-	x
blacklist language of resources	-	x
blacklist file signature	-	x
show **MITRE** matrix	-	x
search **Virustotal** based on strings (*)	-	x
search **MITRE** Technique and Tactics	-	x
classify function groups by colors	-	x
classify strings by groups and by colors	-	x
filter **MITRE** report (full|short)	-	x
filter Indicators Level (1|2|3|4)	-	x
filter **Virustotal** results (all|detected|undetected)	-	x
create XML report file	-	x
command line version of the tool (**pestudiox.exe**)	-	x

* For this search to succeed, you need a valid "Intelligence" account at **Virustotal**.

Please note that the standard version of pestudio may not be used in a professional environment.
Details about the license models: www.winitor.com/tools/pestudio/current/pestudio-licensing.pdf