Static Analysis Tool

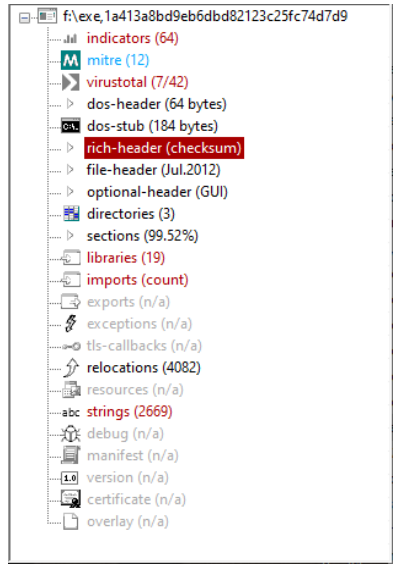
- no installation
- no infection risk
- no sandbox needed
- no expertise required

Features

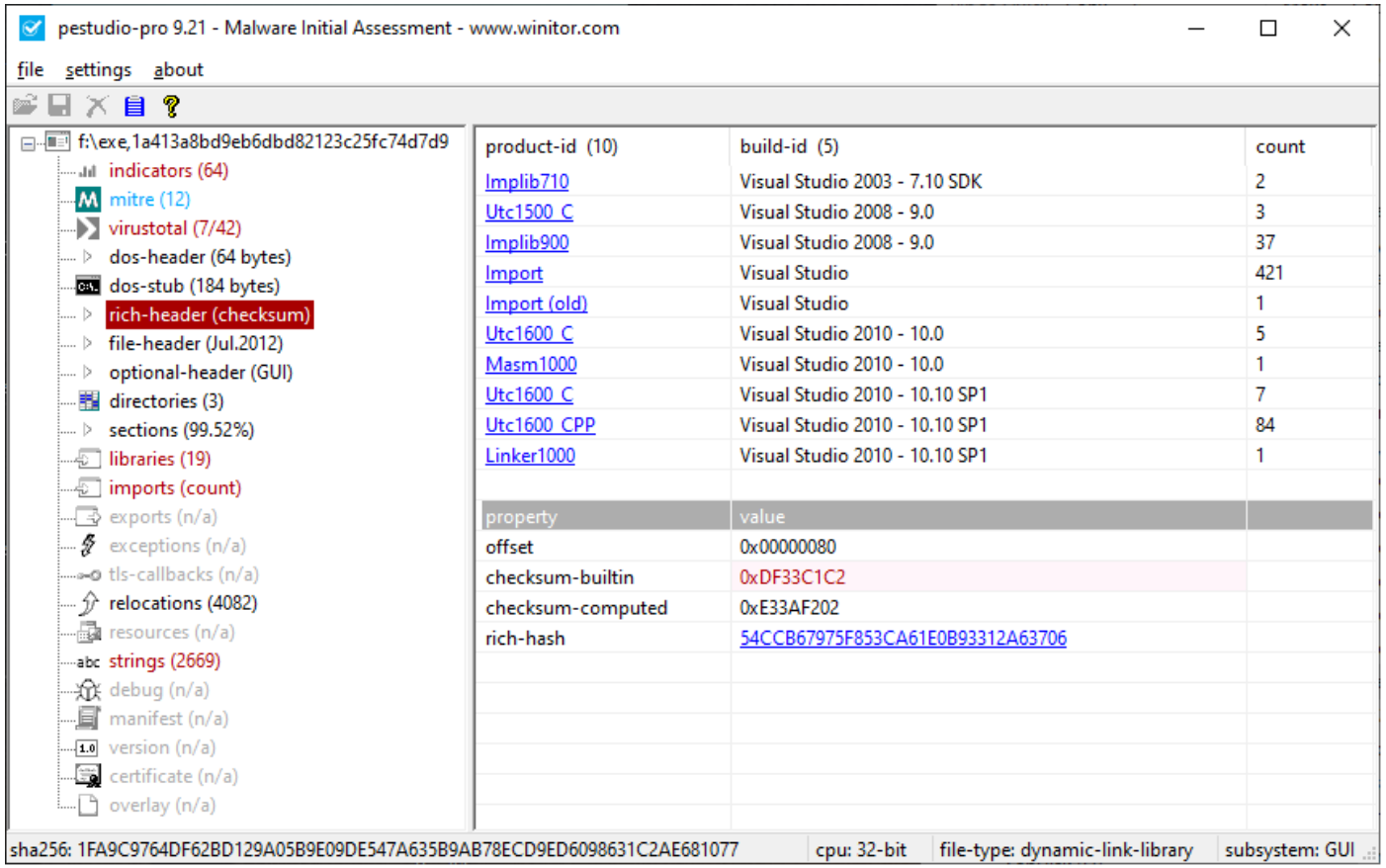
- transform RAW data into information
- spot anomalies
- detect embedded files
- collect imports, exports, strings, resources, ..
- provide hints, indicators, groups, thresholds, ..
- provide @MITREattack indicators
- retrieve scores from @Virustotal
- consume configurations files
- create XML report

Transform RAW data into information

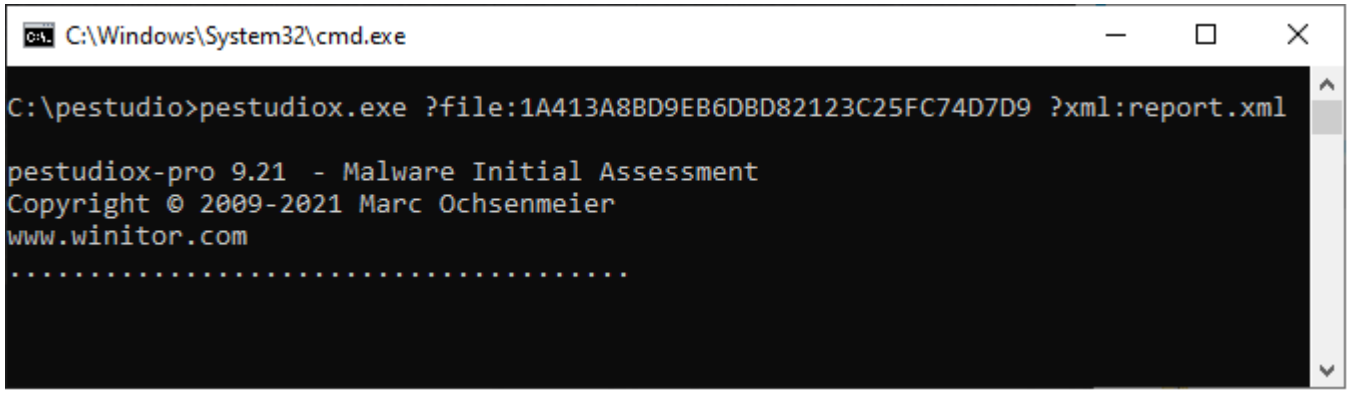
```
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 e800 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
00000080: d092 a7d1 94f3 c982 94f3 c982 94f3 c982  ................
00000090: 9d8b 5a82 8af3 c982 fb97 ca83 97f3 c982  ..Z.............
000000a0: fb97 cd83 83f3 c982 fb97 cc83 91f3 c982  ................
000000b0: fb97 c883 8ff3 c982 94f3 c882 82f2 c982  ................
000000c0: fb97 c183 8df3 c982 fb97 3682 95f3 c982  ..........6.....
000000d0: fb97 cb83 95f3 c982 5269 6368 94f3 c982  ........Rich....
000000e0: 0000 0000 0000 0000 5045 0000 6486 0600  ........PE..d...
```



Interactive Mode



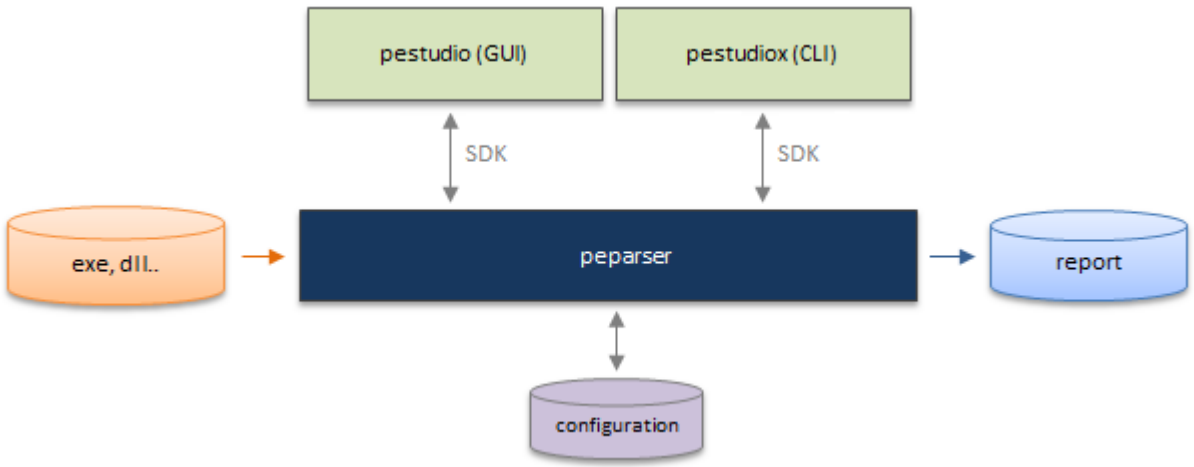
Batch Mode


C:\Windows\System32\cmd.exe
C:\pestudio>pestudiox.exe ?file:1A413A8BD9EB6DBD82123C25FC74D7D9 ?xml:report.xml
pestudiox-pro 9.21 - Malware Initial Assessment
Copyright © 2009-2021 Marc Ochsenmeier
www.winitor.com
.....

Report file

```
<!--pestudio-pro 9.21 - Malware Initial Assessment - www.winitor.com-->
- <image>
  + <overview name="e:\exe,1a413a8bd9eb6dbd82123c25fc74d7d9">
  + <indicators hint="64">
  + <mitre hint="12">
  + <dos-header hint="64 bytes">
  + <dos-stub hint="184 bytes">
  - <rich-header hint="checksum">
      <item count="2" build-id="Visual Studio 2003 - 7.10 SDK" product-id="Implib710"/>
      <item count="3" build-id="Visual Studio 2008 - 9.0" product-id="Utc1500_C"/>
      <item count="7" build-id="Visual Studio 2010 - 10.10 SP1" product-id="Utc1600_C"/>
      <item count="84" build-id="Visual Studio 2010 - 10.10 SP1" product-id="Utc1600_CPP"/>
      <item count="1" build-id="Visual Studio 2010 - 10.10 SP1" product-id="Linker1000"/>
    </rich-header>
  + <file-header hint="Jul.2012 ">
  + <optional-header hint="GUI">
  + <directories hint="3">
  + <sections hint="99.52%">
  + <libraries hint="19">
  + <imports hint="420">
    <exports>n/a</exports>
  + <relocations count="4082">
</image>
```

Architecture



Flexible configuration