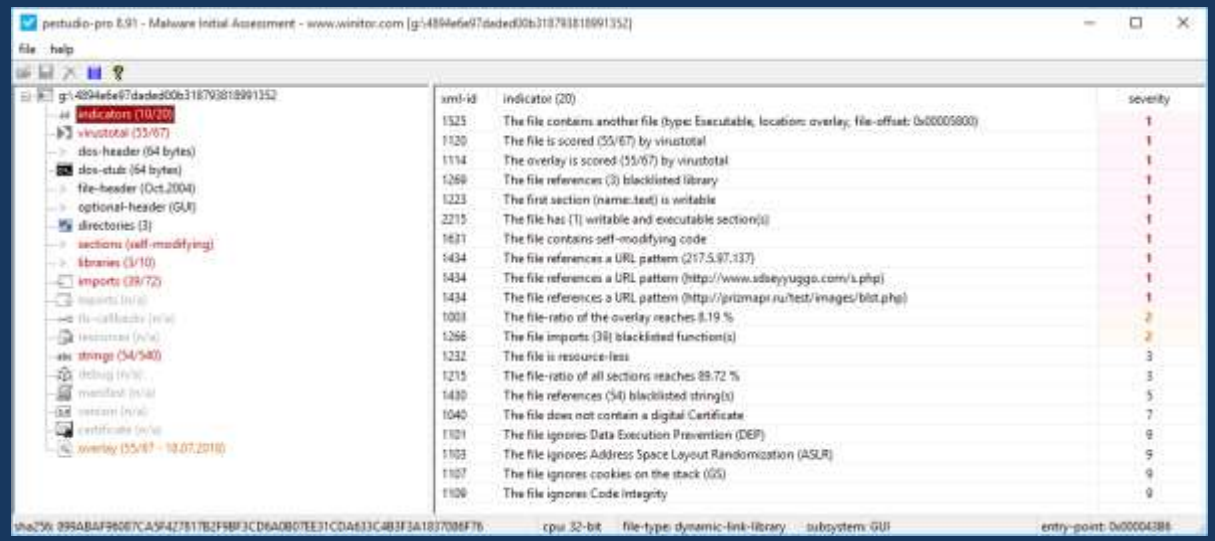
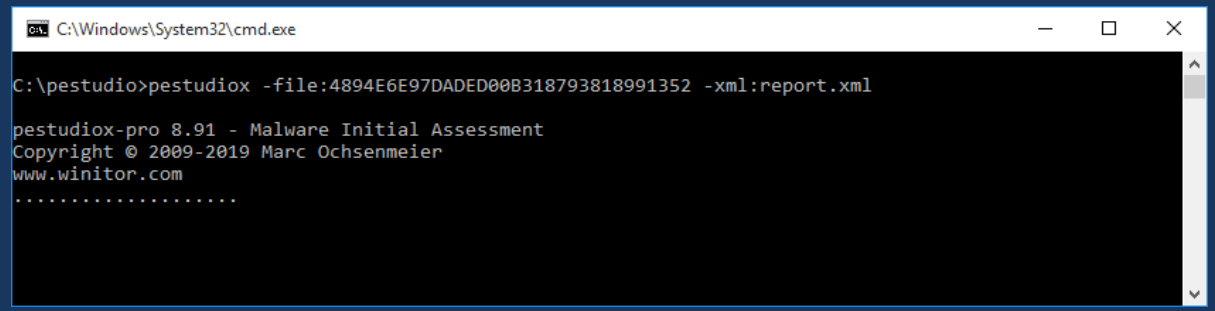
pestudio

Malware Initial Assessment





Features

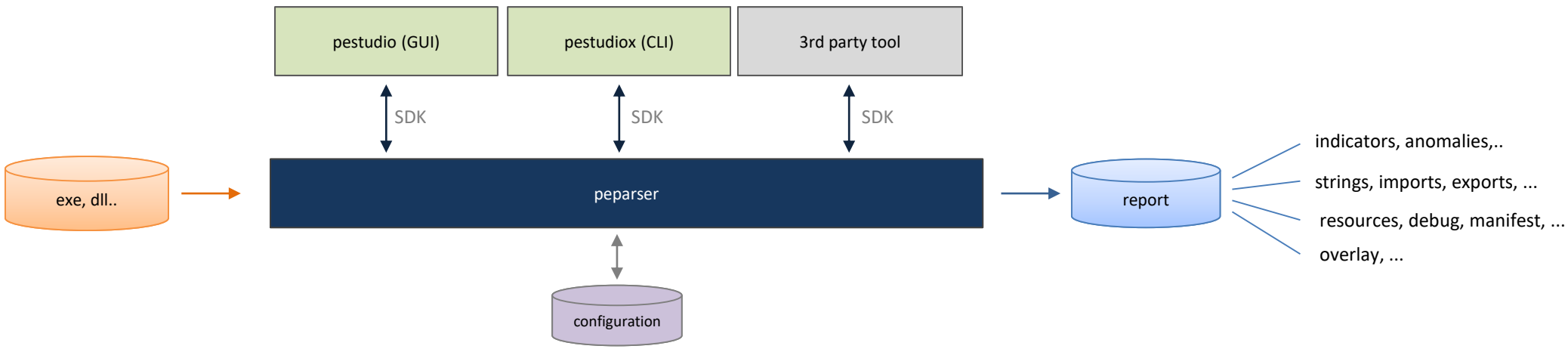
- show potential
- spot anomalies
- verify thresholds
- find embedded files
- collect hints
- provide indicators
- export report
- consume filters
- retrieve scores from @virustotal

Characteristics

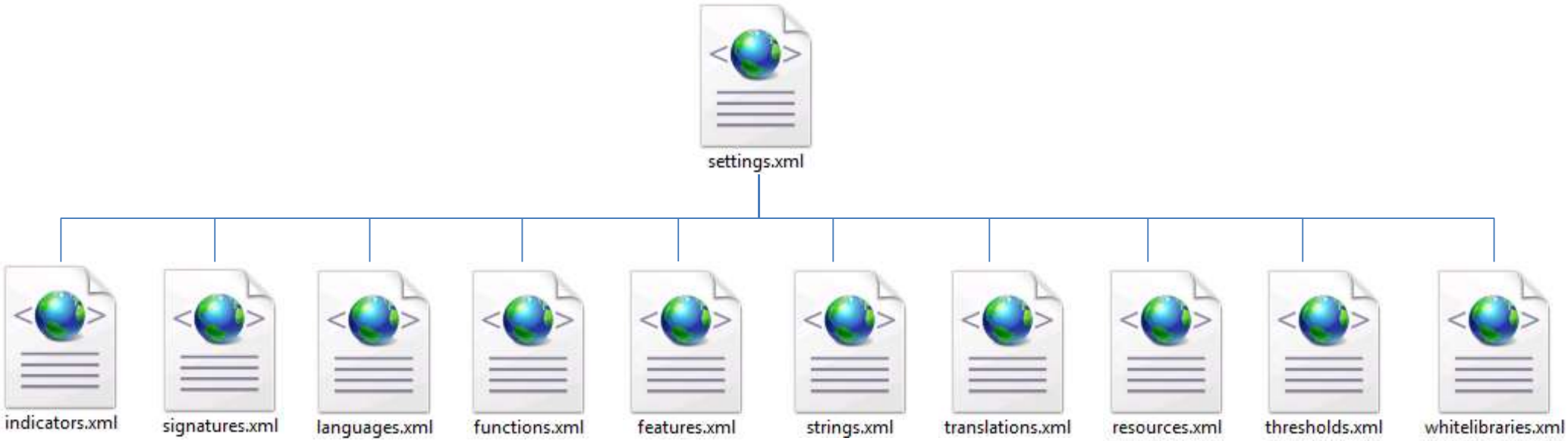
- zero footprint
- no installation
- no infection risk
- no sandbox needed
- low expertise required

Architecture

- GUI & CLI clients
- RAW parser server
- Flexible configuration



Flexible configuration



Report file

- share IOCs
- integrate into tools-chain

```
<?xml version="1.0" encoding="UTF-8"?>
<!--pestudio-pro 8.91 - Malware Initial Assessment - www.winitor.com-->
- <image>
  - <overview name="f:\md5,0615f7495fb73503d83c354c3021325a">
      <description>n/a</description>
      <file-version>n/a</file-version>
      <file-type>dynamic-link-library</file-type>
      <cpu>32</cpu>
      <size>20992</size>
      <size-without-overlay>n/a</size-without-overlay>
      <subsystem>GUI</subsystem>
      <signature>n/a</signature>
      <entropy>6.048</entropy>
      <compiler-stamp>Tue Aug 16 18:40:11 2016 </compiler-stamp>
      <debugger-stamp>Tue Aug 16 18:40:11 2016 </debugger-stamp>
      <resources-stamp>n/a</resources-stamp>
      <exports-stamp>Tue Aug 16 18:40:11 2016 </exports-stamp>
      <version-stamp>n/a</version-stamp>
      <entry-point-hex>8B FF 55 8B EC 83 7D 0C 01 75 05 E8 F1 03 00 00 5D </entry-point-hex>
      <first-bytes-hex>4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 </first-bytes-hex>
      <first-bytes-text>M Z .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. </first-bytes-text>
      <md5>0615F7495FB73503D83C354C3021325A</md5>
      <md5-without-overlay>n/a</md5-without-overlay>
      <sha1>758B745FAEB610F148550817AD66F4CF683F23B9</sha1>
      <sha1-without-overlay>n/a</sha1-without-overlay>
      <sha256>19DE921E3E862B5CF87DC5D378749E0752BAD54BB6F432474668942BF7DCE2E1</sha256>
      <sha256-without-overlay>n/a</sha256-without-overlay>
      <imphash>n/a</imphash>
    </overview>
  + <indicators severity="1" count="16">
    <virustotal>offline</virustotal>
  + <dos-header hint="64 bytes">
  + <dos-stub hint="!This program cannot be run in DOS mode.">
  + <file-header hint="Aug.2016 ">
  + <optional-header hint="GUI">
  + <directories count="6">
  + <sections file-ratio="95.12%">
  + <libraries count="7" blacklist="1">
  + <imports count="59" blacklist="7">
  + <exports count="4">
  + <debug hint="path">
    <version>n/a</version>
  + <strings count="339" bl="17">
</image>
```

Demo