malware analysis

**02 - Detecting packing and obfuscation**

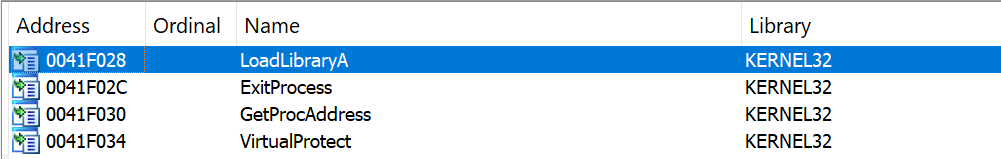
# Lesson 02 LAB solutions

Total point values of this lab: 20 points. Point value is assigned by each task below.

### **Lab exercise 1:**

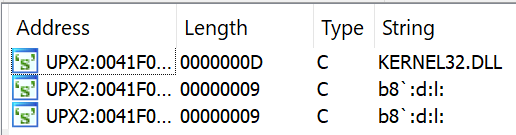
*Learning Outcomes 1, 2, 3 and 4*

1. Based off the imports table this sample appears to be packed.



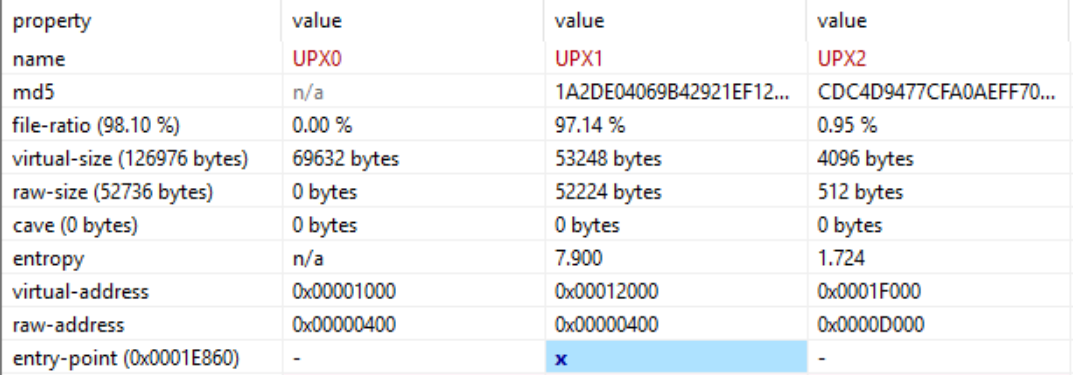
These are the only imported functions, the LoadLibrary and GetProcAddress functions are signature imports for packed PE files. This screenshot was produced by IDA Pro.

1. Again, based off the dumped strings, the sample appears to be packed.



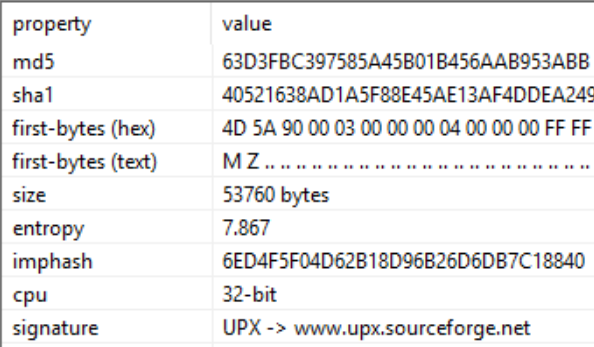
There are only 3 strings in the sample and one of them is the name of a dll that is used by the program. This is not typical of normal executables. This screenshot was produced by IDA Pro.

1. The sections table is not normal. The names of the sections are: UPX0, UPX1, and UPX2. UPX0 has a size of 0.



As seen, the table values are non-standard. This screenshot was taken of pestudio.

1. This sample is packed based off the first two questions and the fact that when opened, IDA warned that the sample could be packed.

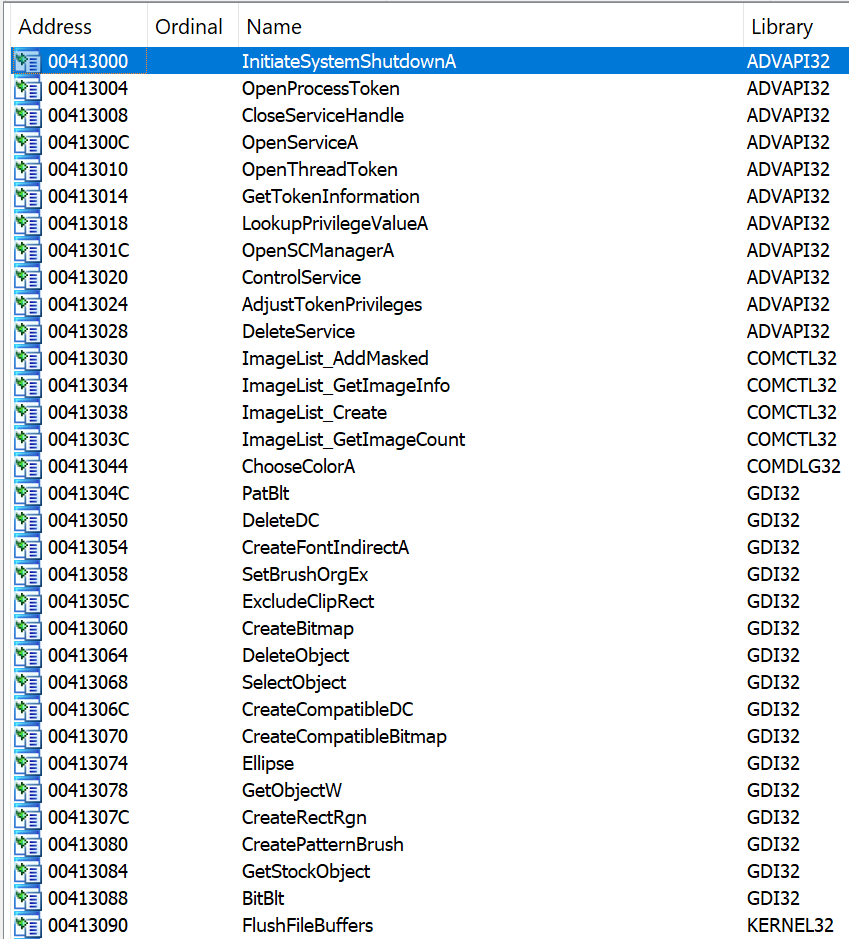


Pestudio will also identify the signature to be the UPX packer, as seen at the bottom of the screenshot.

### **Lab Exercise 2:**

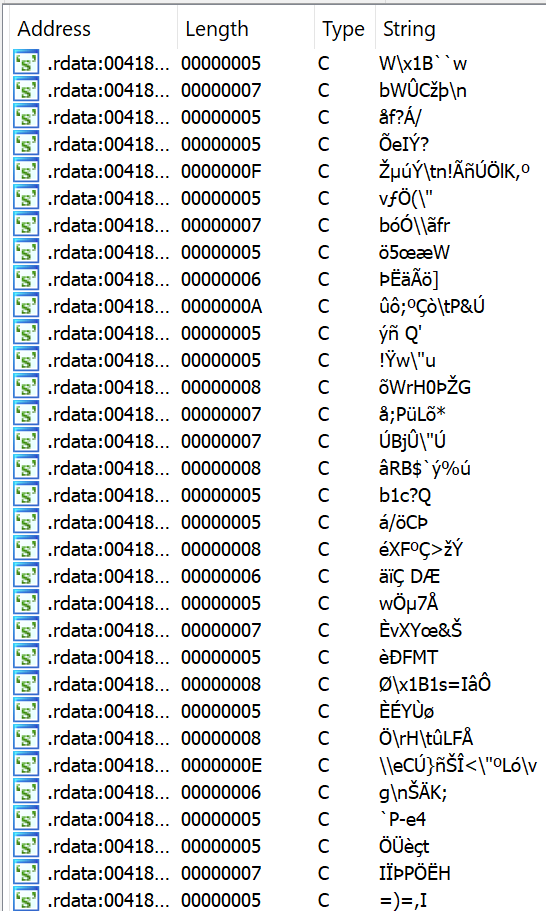
*Learning Outcomes 1, 2, 3 and 4*

1. Based off the imports table this sample does not appear to be packed.



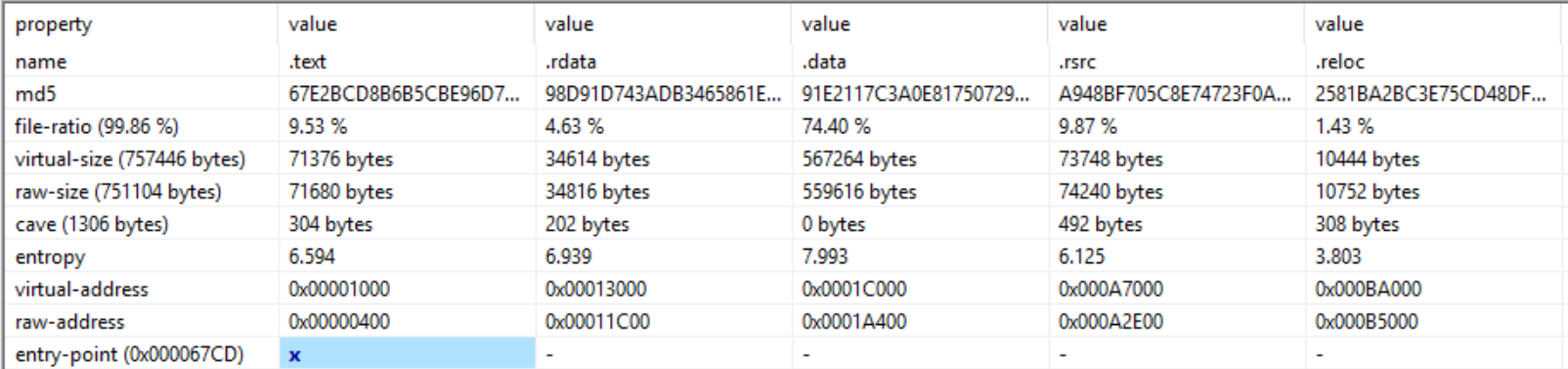
There are many imports in this sample that do not deal with packers. This screenshot was produced by IDA Pro.

1. Again, based off the dumped strings, does not appear to be packed. However, it does look to be obfuscated.



There are many strings which leads to the conclusion that the sample is not packed. The strings are very random and do not appear to contain any plain text data. This screenshot was produced by IDA Pro.

1. The sections table of this sample appears to be normal. The section sizes have standard names and sizes.



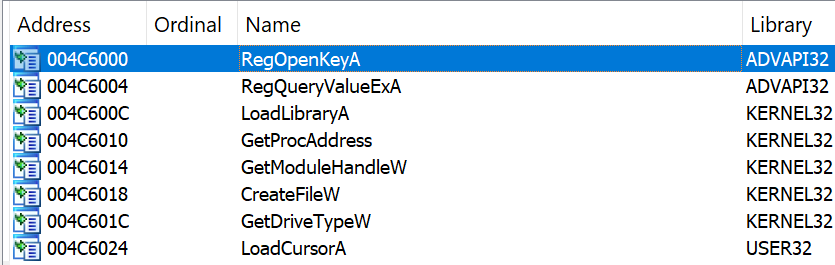
As seen, the table values are standard and the sizes are normal. This screenshot was taken of pestudio.

1. Based off the above answers the sample does not look to be packed. It is obfuscated though because the strings appear highly random.

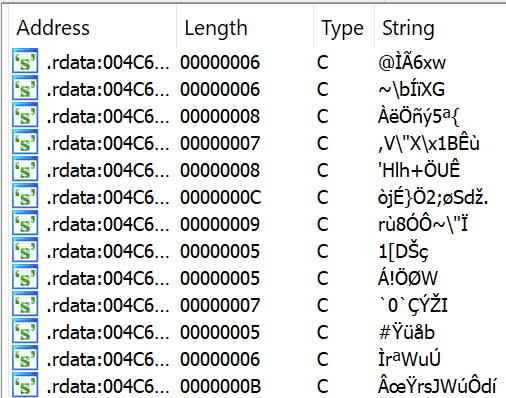
### **Lab Exercise 3:**

*Learning Outcomes 1, 2, 3 and 4*

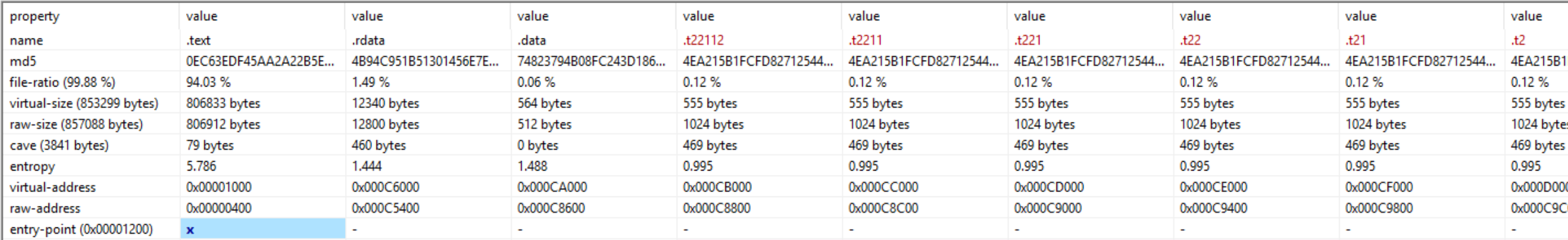
1. This program is not immediately identified as packed. IDA opens it without any warnings. It does have few imports:



And the strings don’t appear to be normal:



The sections table is non-standard as well:



The naming scheme and the section sizes suggest that the sample could be packed.