how to Deal with Packed Binaries

how to Deal with Packed Binaries

TO pack or Not to Pack

Packing : It just Compression For a already Know Malware To change it signature

EX: **UPX (Very Famous packing Program)**

Size will Also Decrease , Will have a very tiny code , **it will be Extracted at runtime**.

So , When you Deal with a packed library.

It will Use `LoadLibrary` and `GetProcAddress` API Calls to load all the Api Then it will inflate back to its original size.

Now Size of raw data and virtual size will differ by a big amount.

Now Basics of Static analyis is done.
We can Use PEStudio for all the things we have learned.