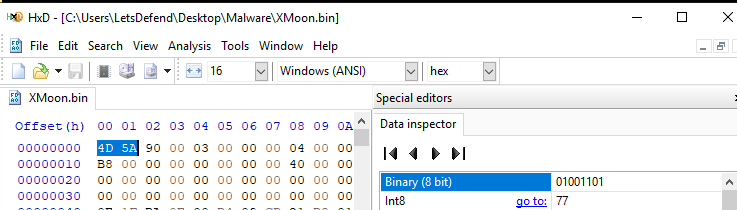
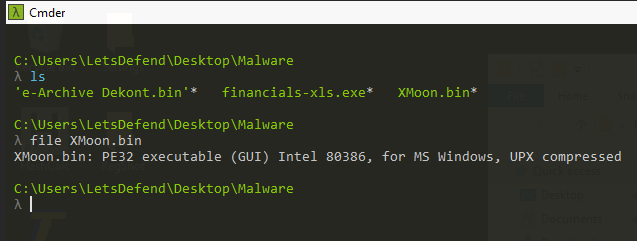
In this example, I will be examining a piece of malware “Xmoon.bin” using a virtual environment of Flare-VM.

What is the actual extension of the "XMoon.bin" file?

To find the actual extension of the “XMoon.bin” file, I will use the application “HxD”. Within the first line are the keywords “4D 5A” which are the file signatures for an exe file.



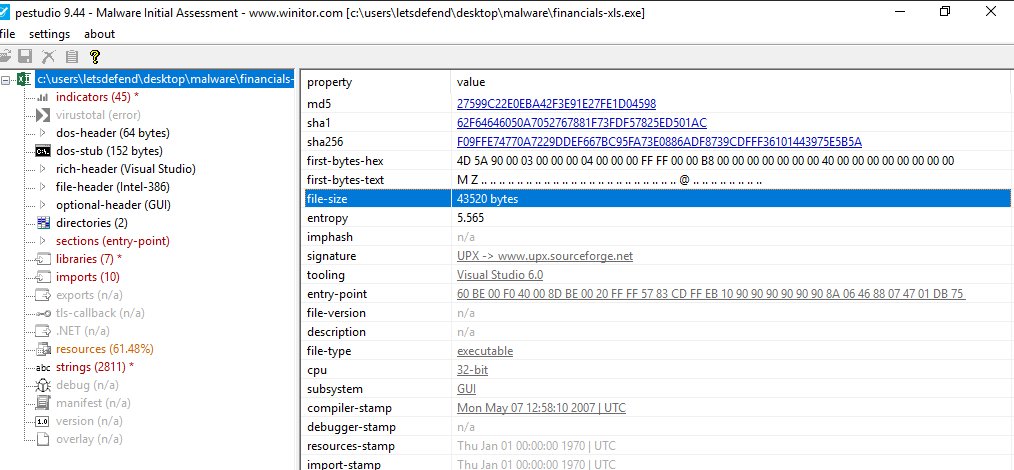
Another way to check the file extension is by using the Cmder application using the file command. As shown XMoon.bin is a PE32 executable file or exe.



What are the first 4 characters you will see when you open the XMoon.bin file with the Hex editor? (Do not put spaces between characters.)

4D5A  
  
 What is the signature value of "financials-xls" file?

Using the application pestudio, I can find the alot of data on the “financial-xls” file including its digital signature of “UPX -> [www.upx.sourceforge.net](http://www.upx.sourceforge.net)”



What is the actual file size of the "financials-xls" file? (byte)

The actual file size of 53,520 bytes can be found in pestudio or by right lciking on properties for the file.