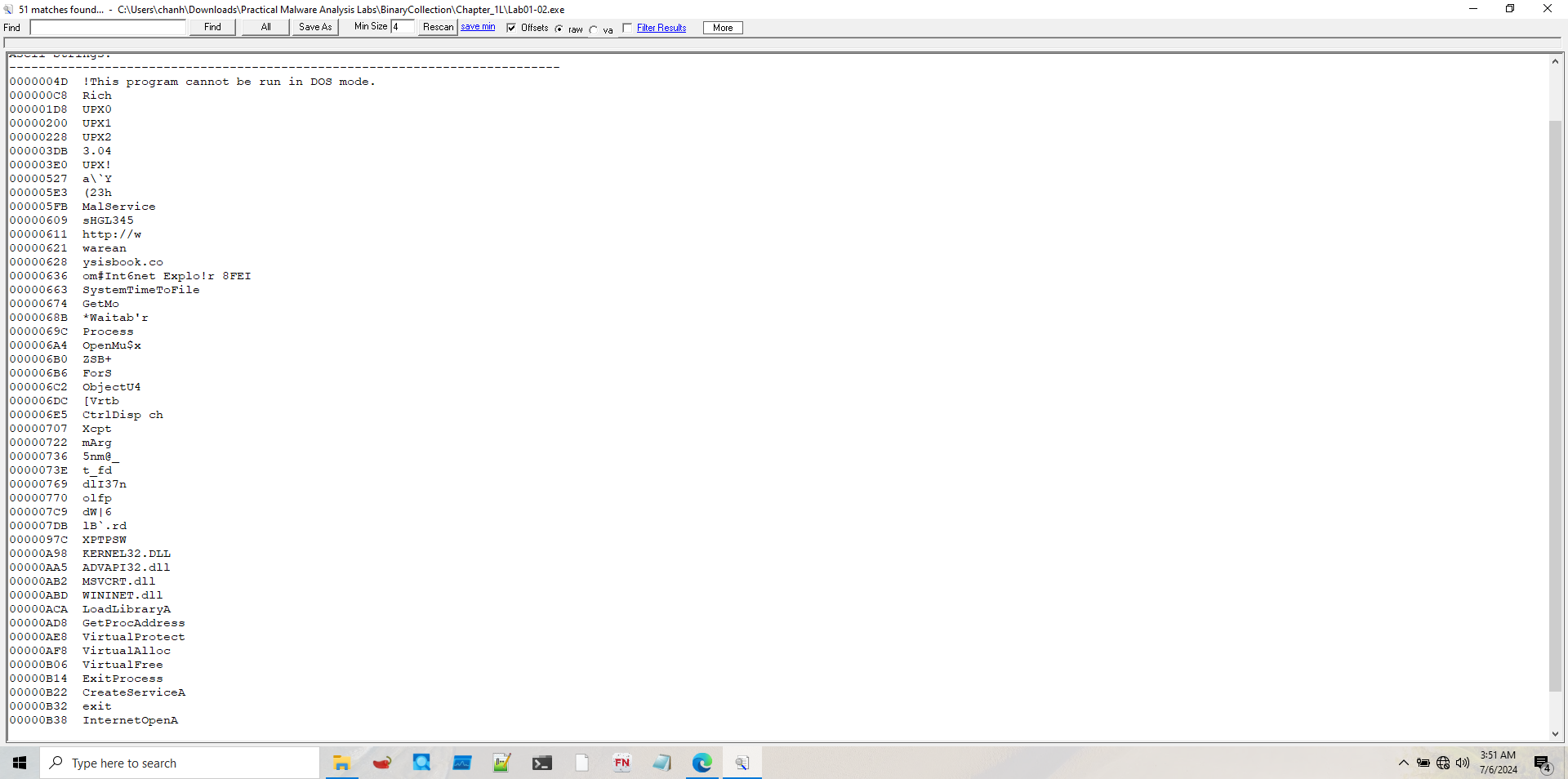
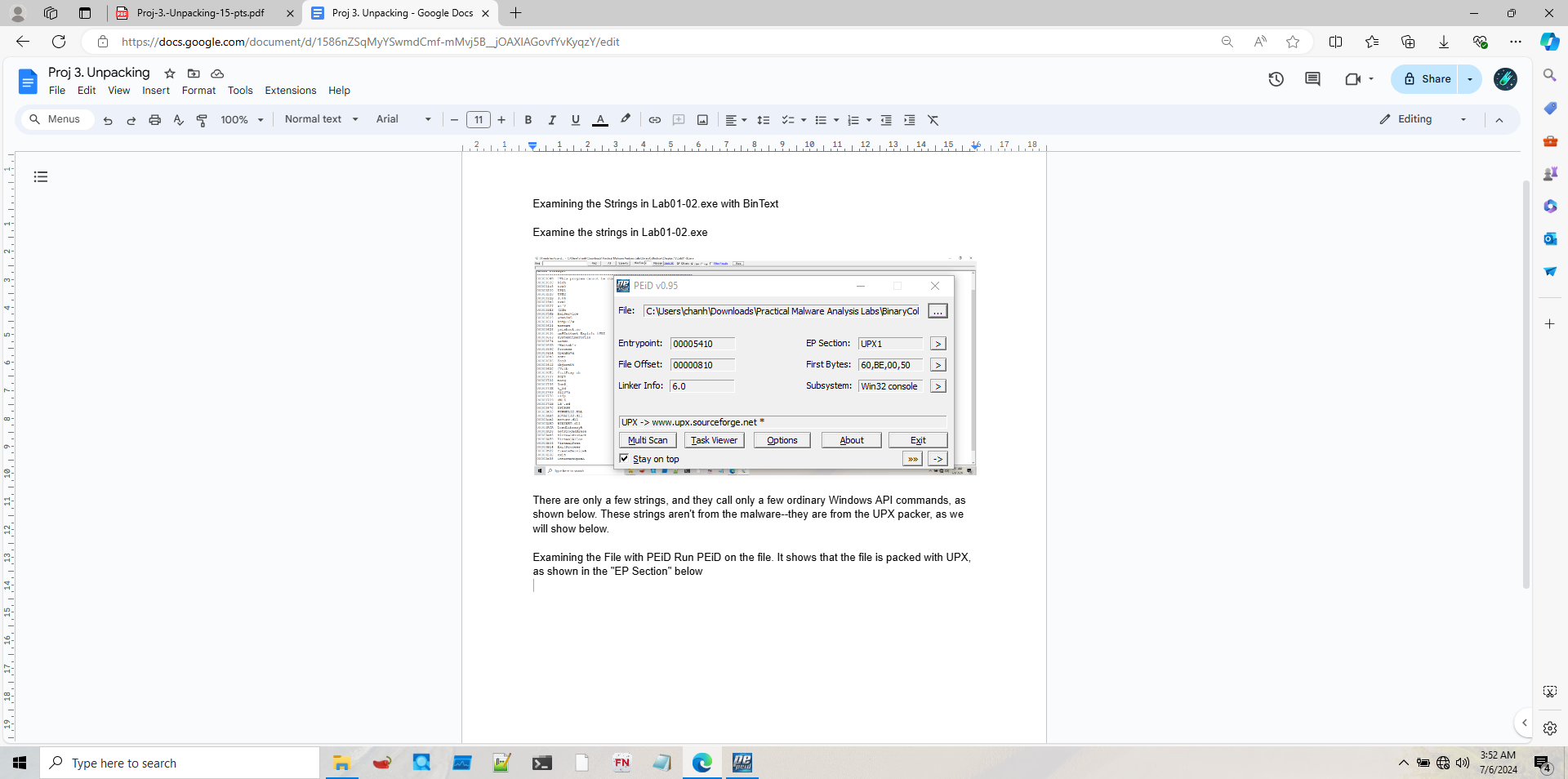
Examining the Strings in Lab01-02.exe with BinText

Examine the strings in Lab01-02.exe



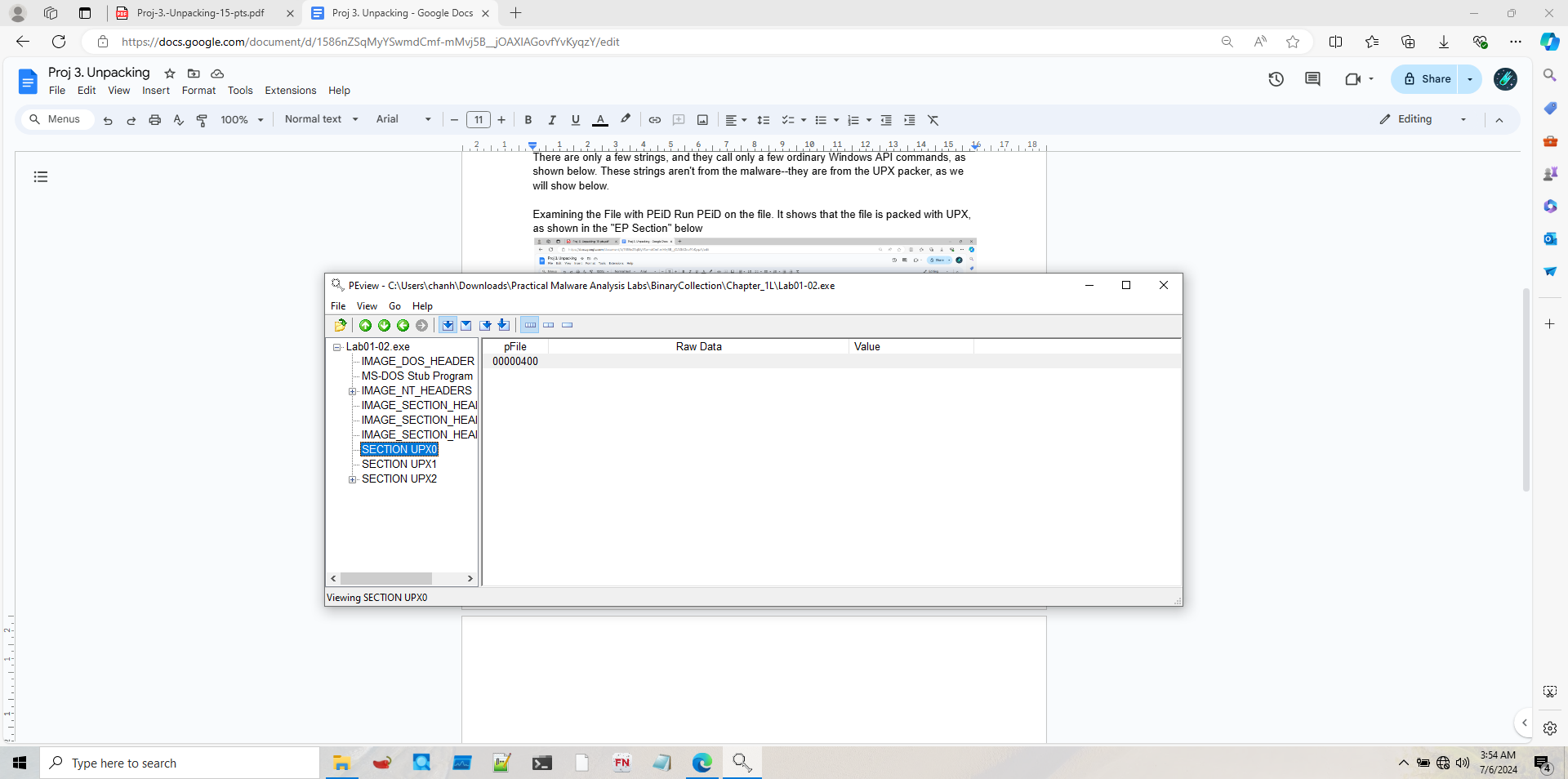
There are only a few strings, and they call only a few ordinary Windows API commands, as shown below. These strings aren't from the malware--they are from the UPX packer, as we will show below.

Examining the File with PEiD Run PEiD on the file. It shows that the file is packed with UPX, as shown in the "EP Section" below



Examining the File with PEview Run PEview on the file.

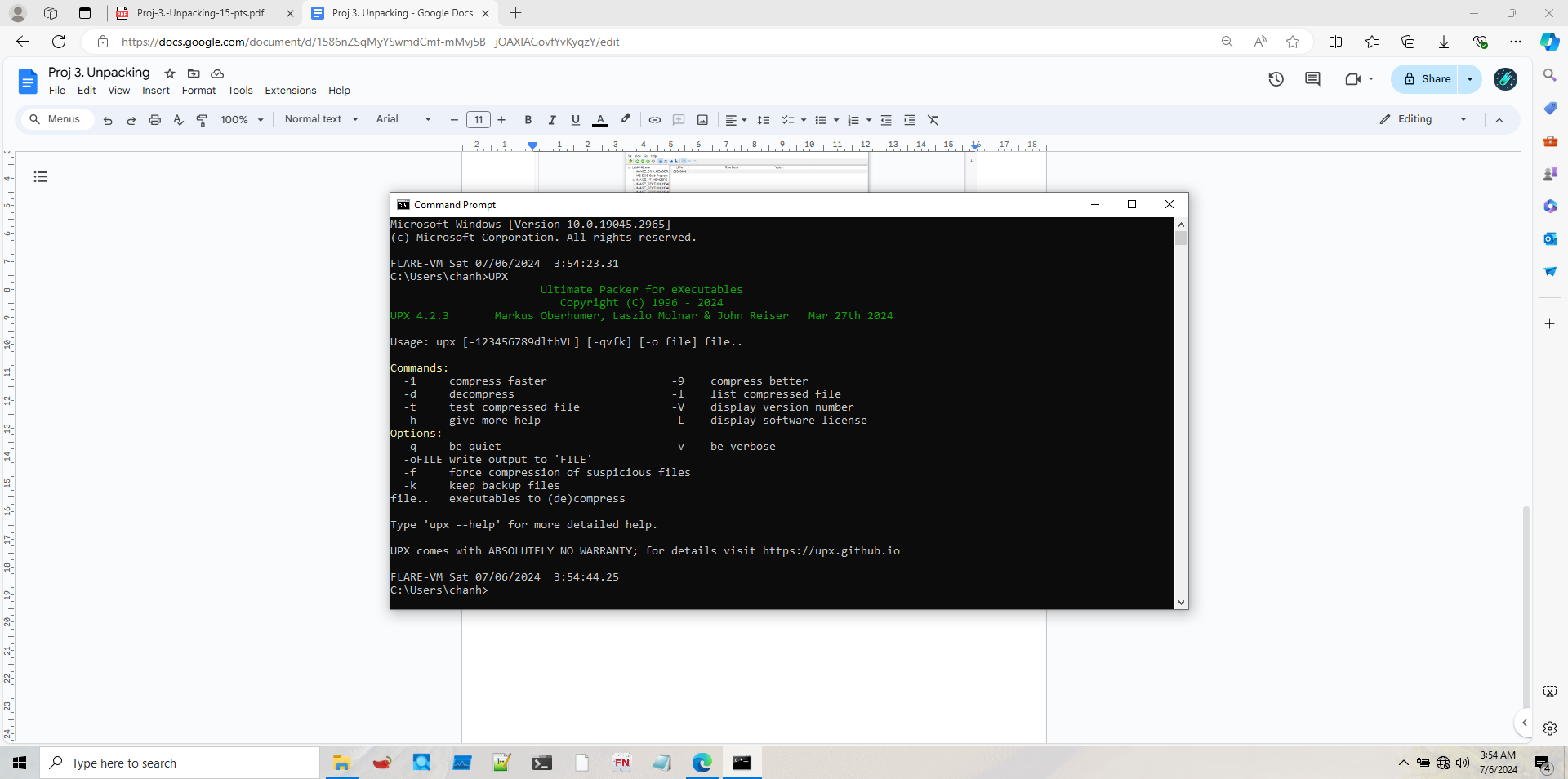
The file has sections labeled UPX0, UPX1, and UPX2, as shown below. These are section names produced by the UPX packer.



Unpacking the File with UPX

Open a Command Prompt window and execute this command

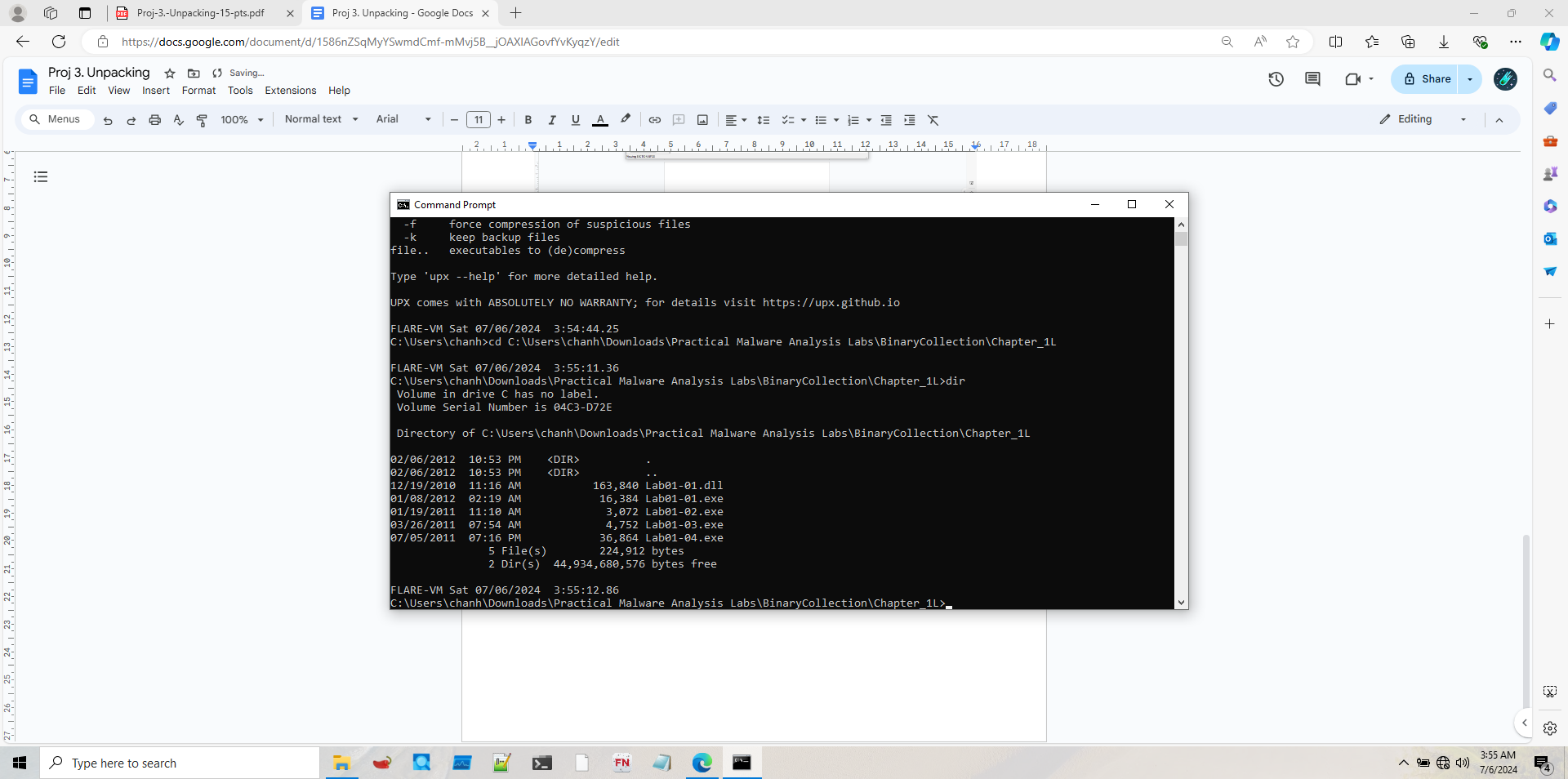
UPX



Execute these commands to move to the directory containing the malware samples, and list the files there

cd "\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter\_1L"

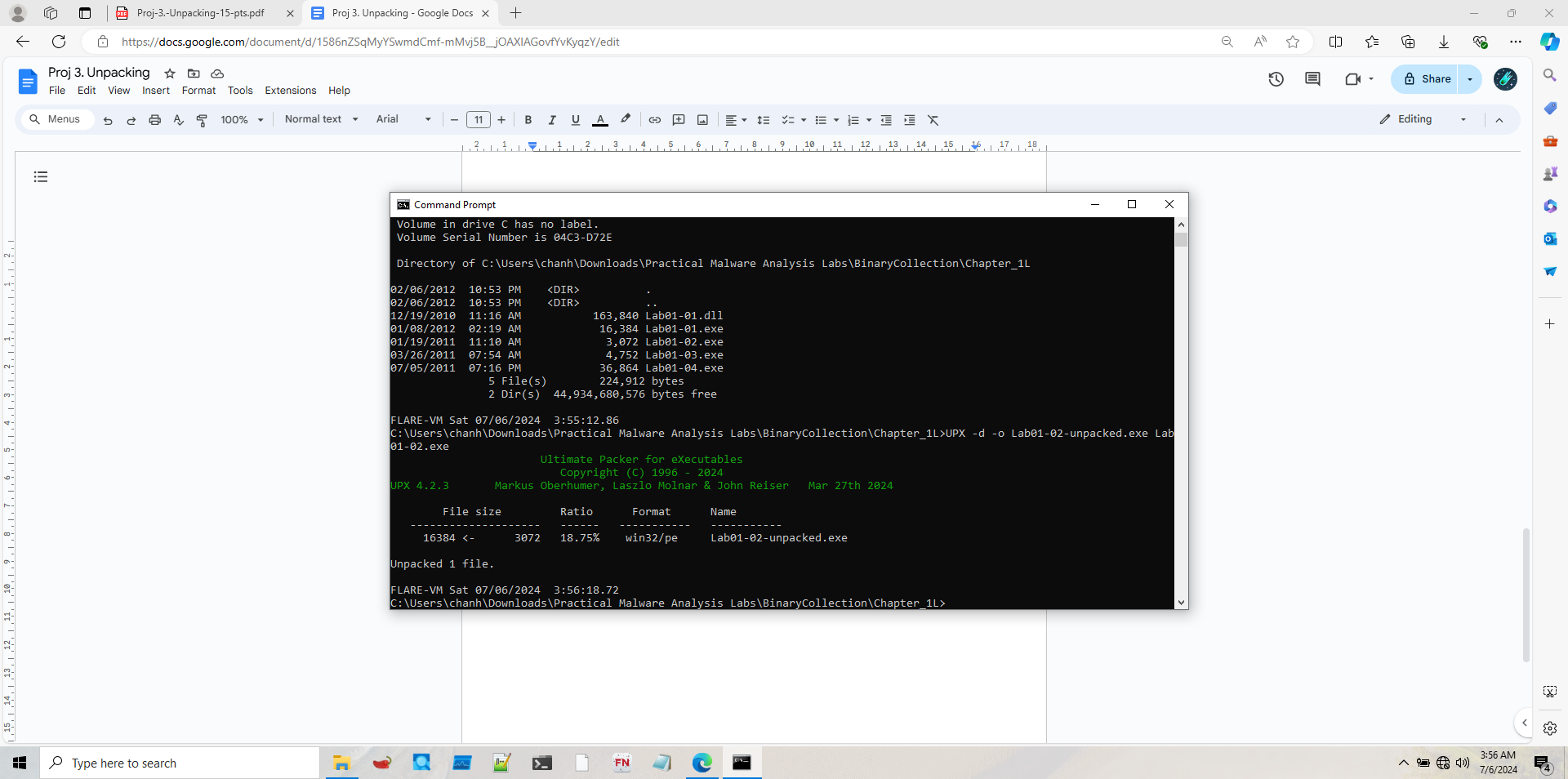
Dir



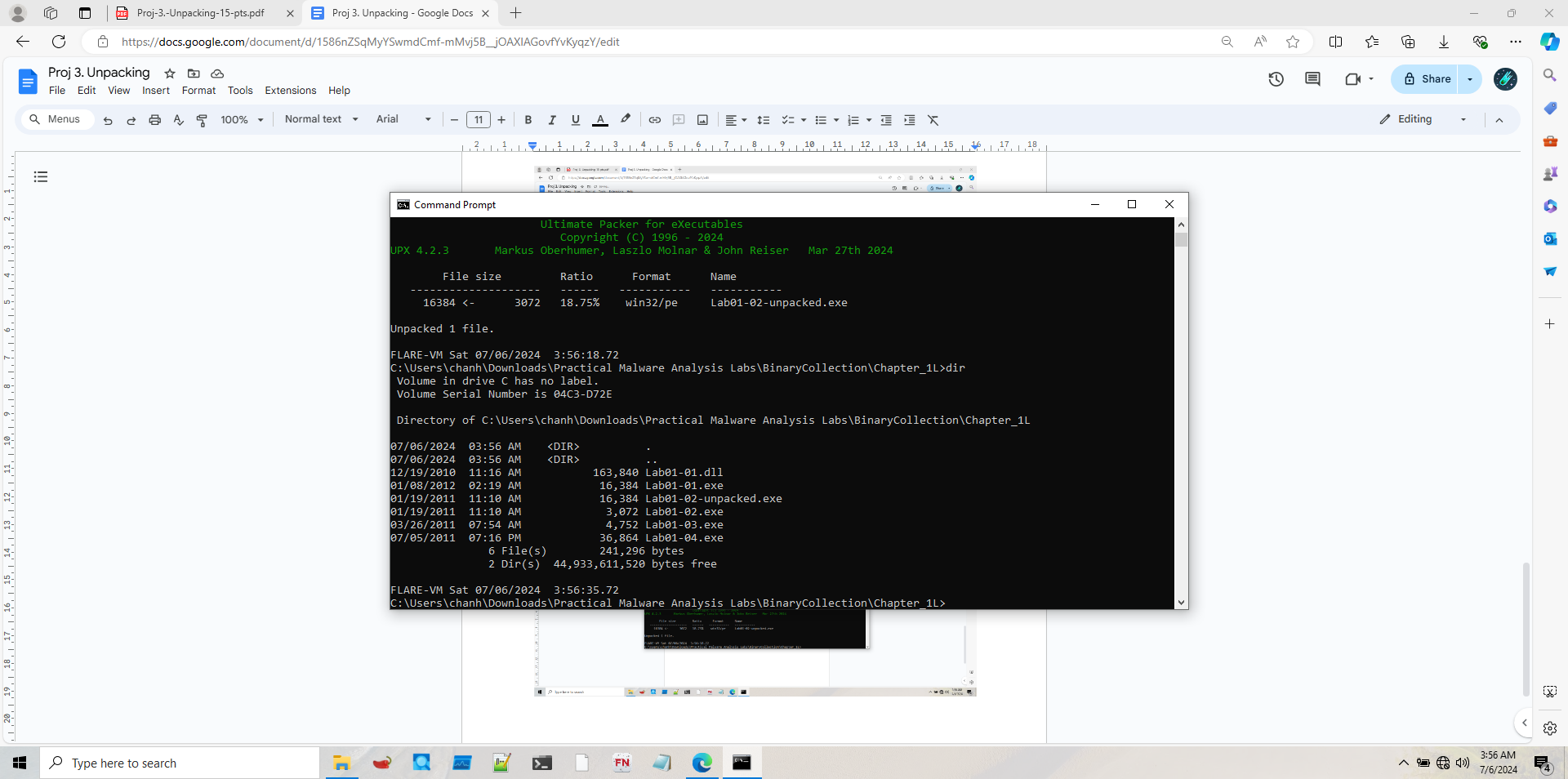
Execute these commands to unpack the file, and list the files again:

UPX -d -o Lab01-02-unpacked.exe Lab01-02.ex

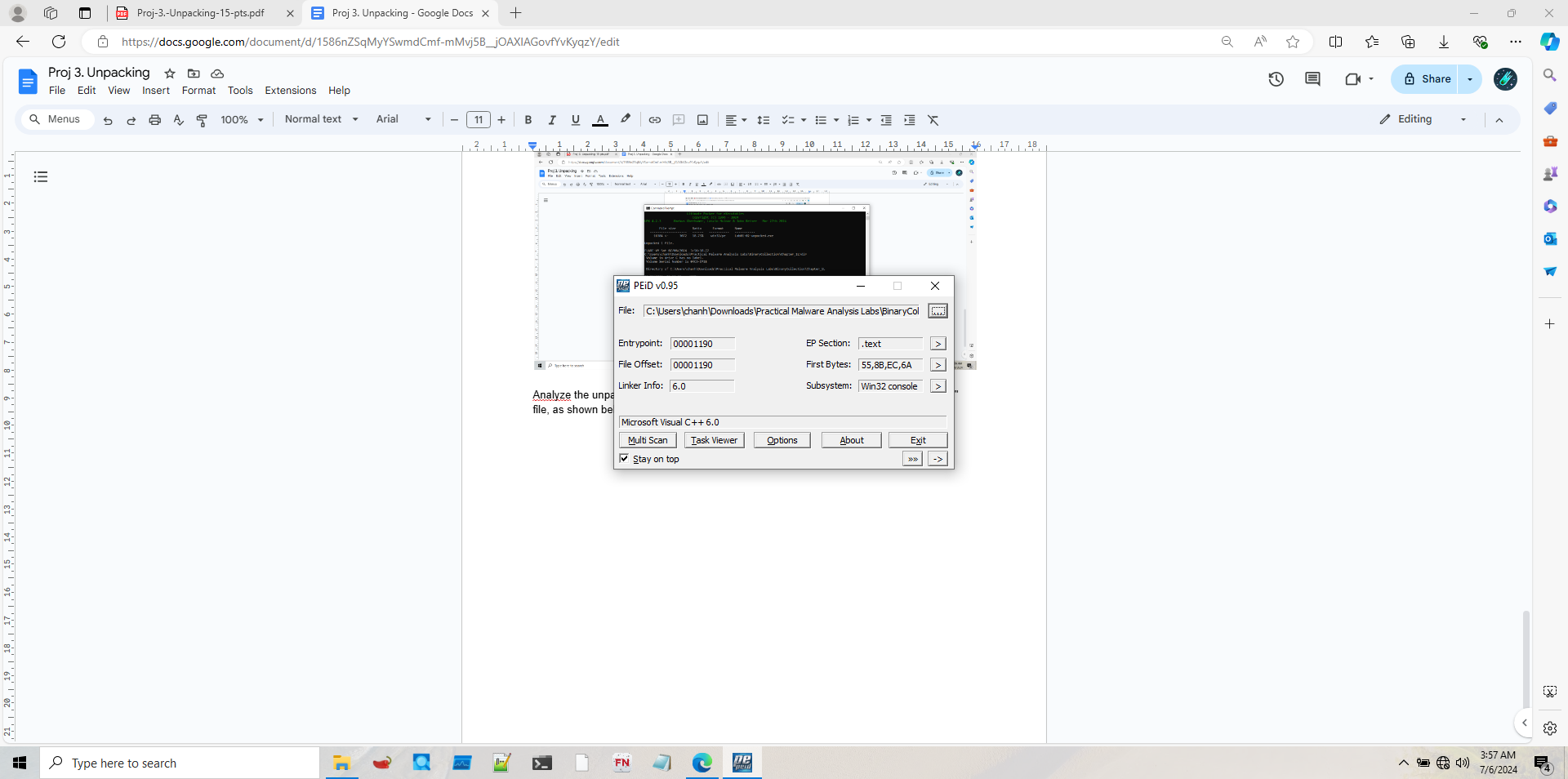
Dir



The unpacked file is much larger than the original file, as shown below



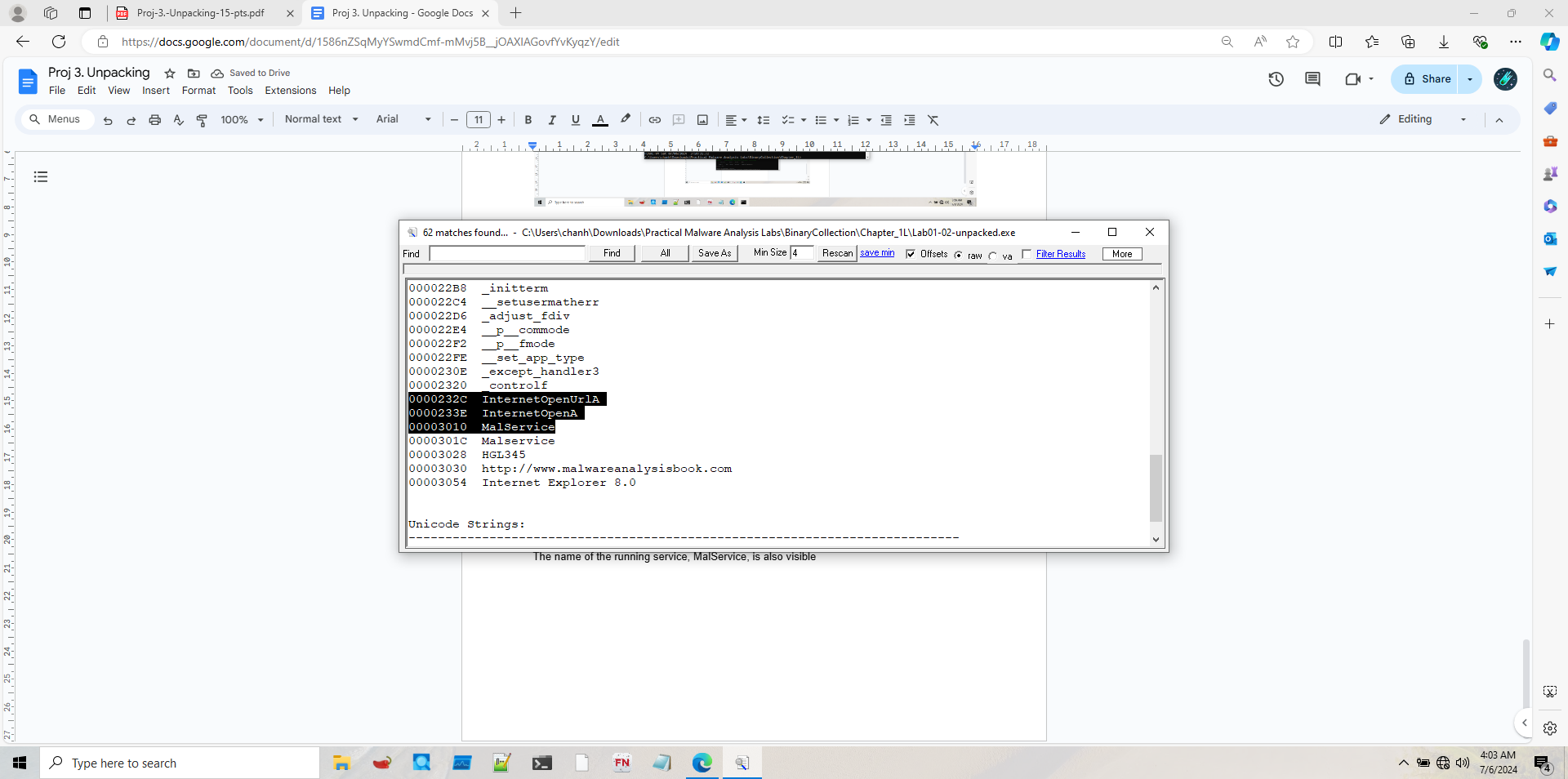
Analyze the unpacked file with PEiD. It now is regognized as a "Microsoft Visual C++ 6.0" file, as shown below



Find the strings in the unpacked file

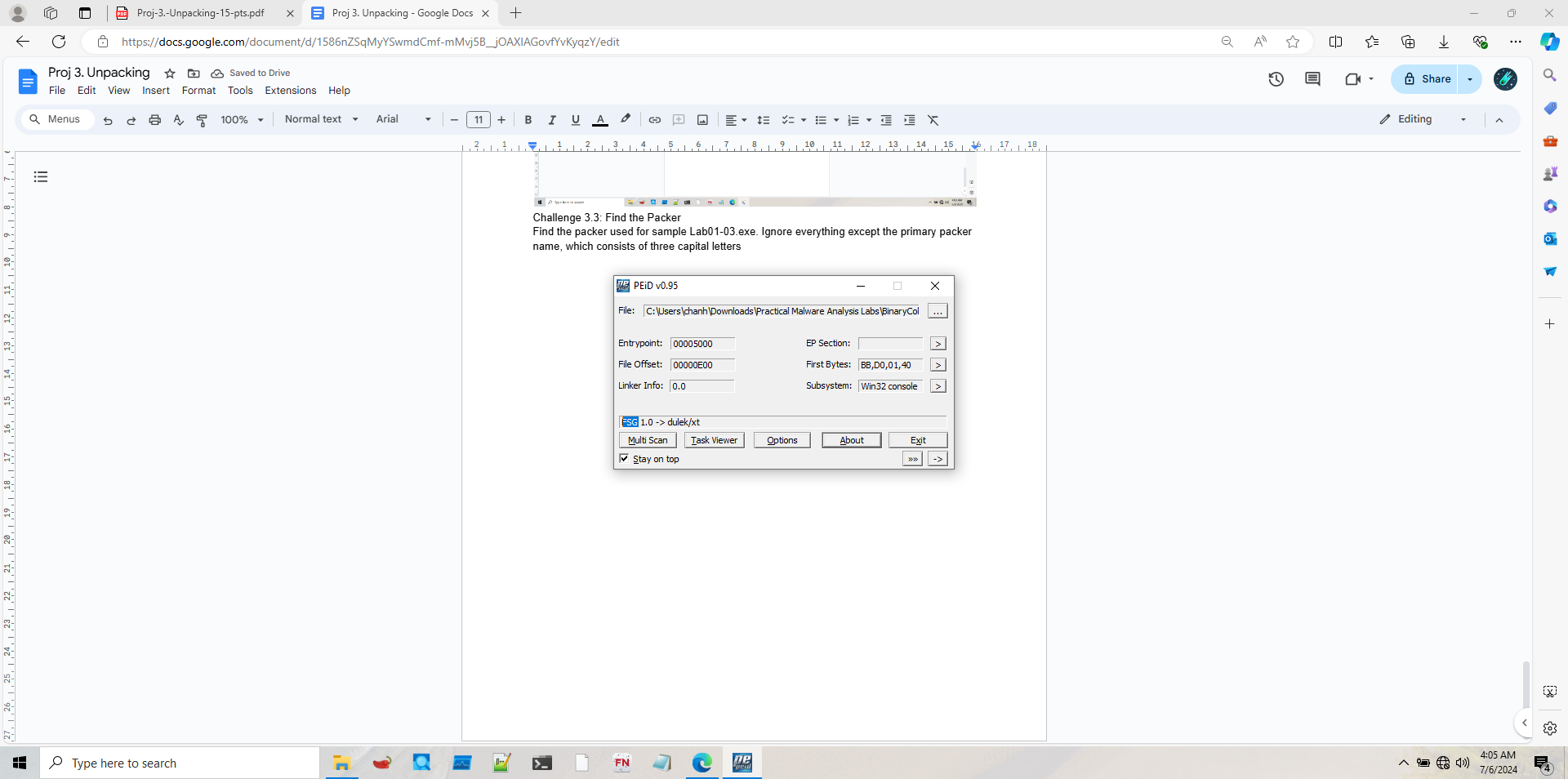
You should see the API names InternetOpenURLA and InternetOpenA, and the Command-and-Control URL http://www.malwareanalysisbook.com, as shown below.

These suggest that infected machines will connect to http://www.malwareanalysisbook.com. The name of the running service, MalService, is also visible



Challenge 3.3: Find the Packer

Find the packer used for sample Lab01-03.exe. Ignore everything except the primary packer name, which consists of three capital letters



FSG