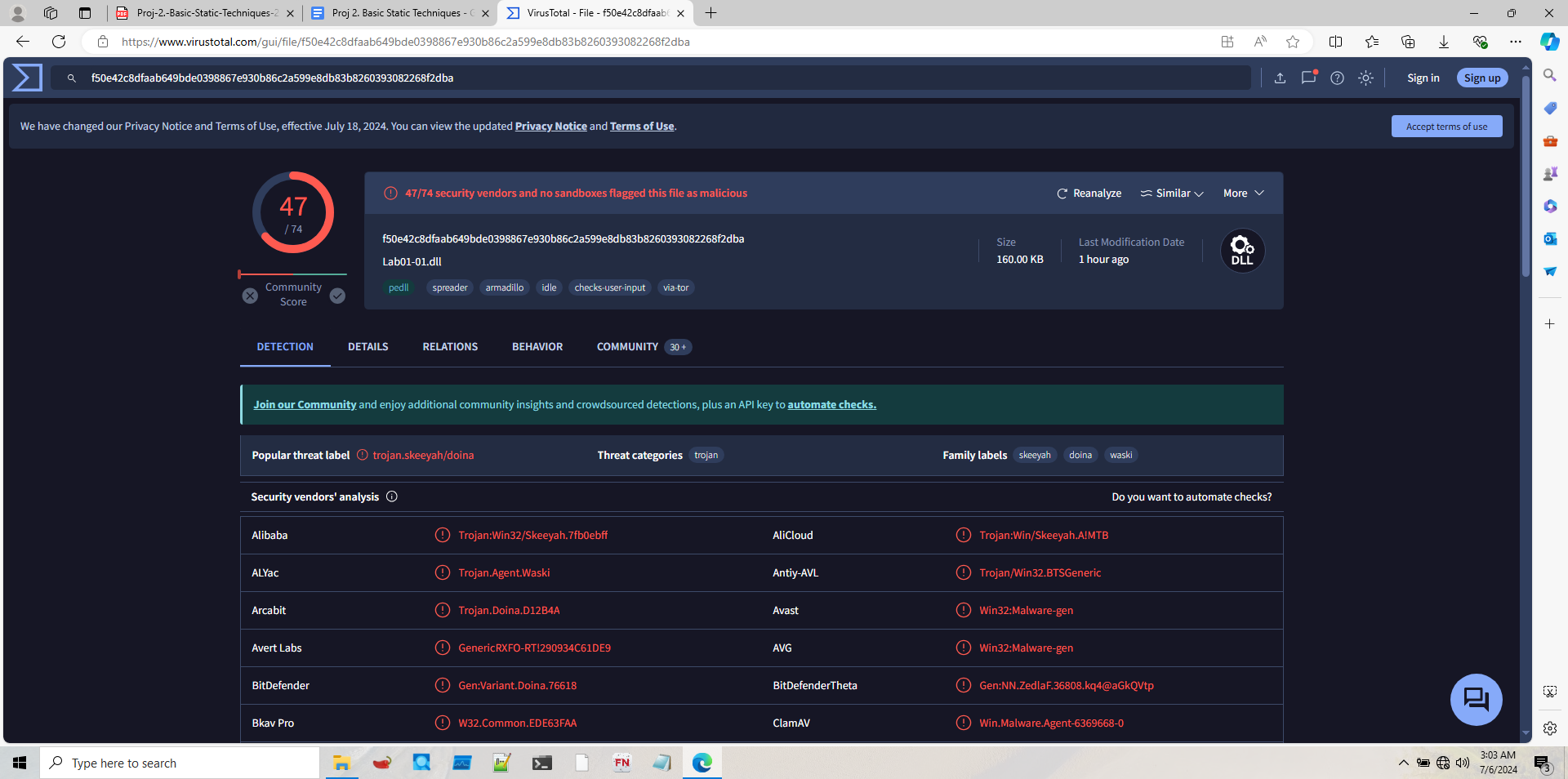
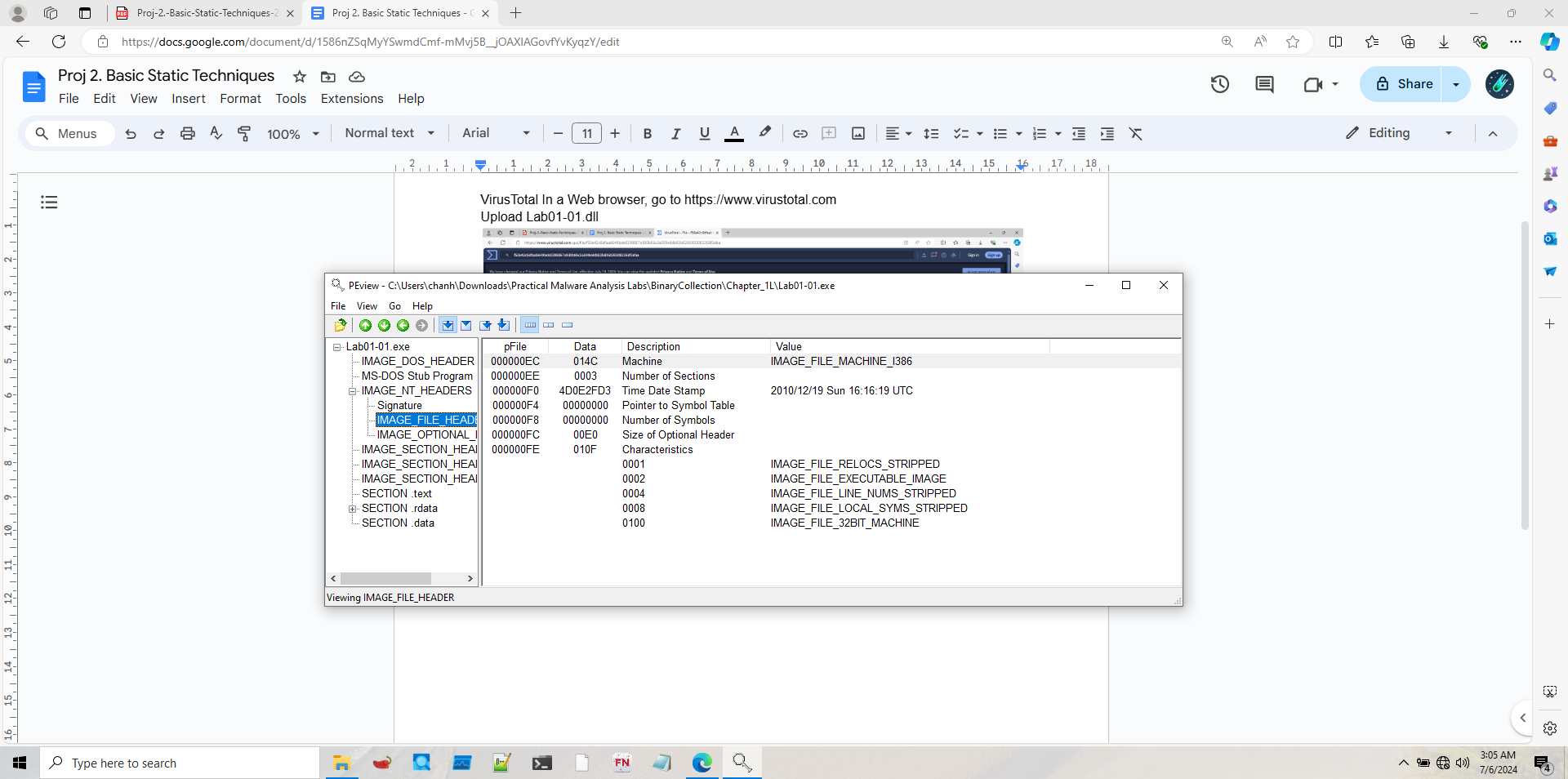
VirusTotal In a Web browser, go to https://www.virustotal.com

Upload Lab01-01.dll

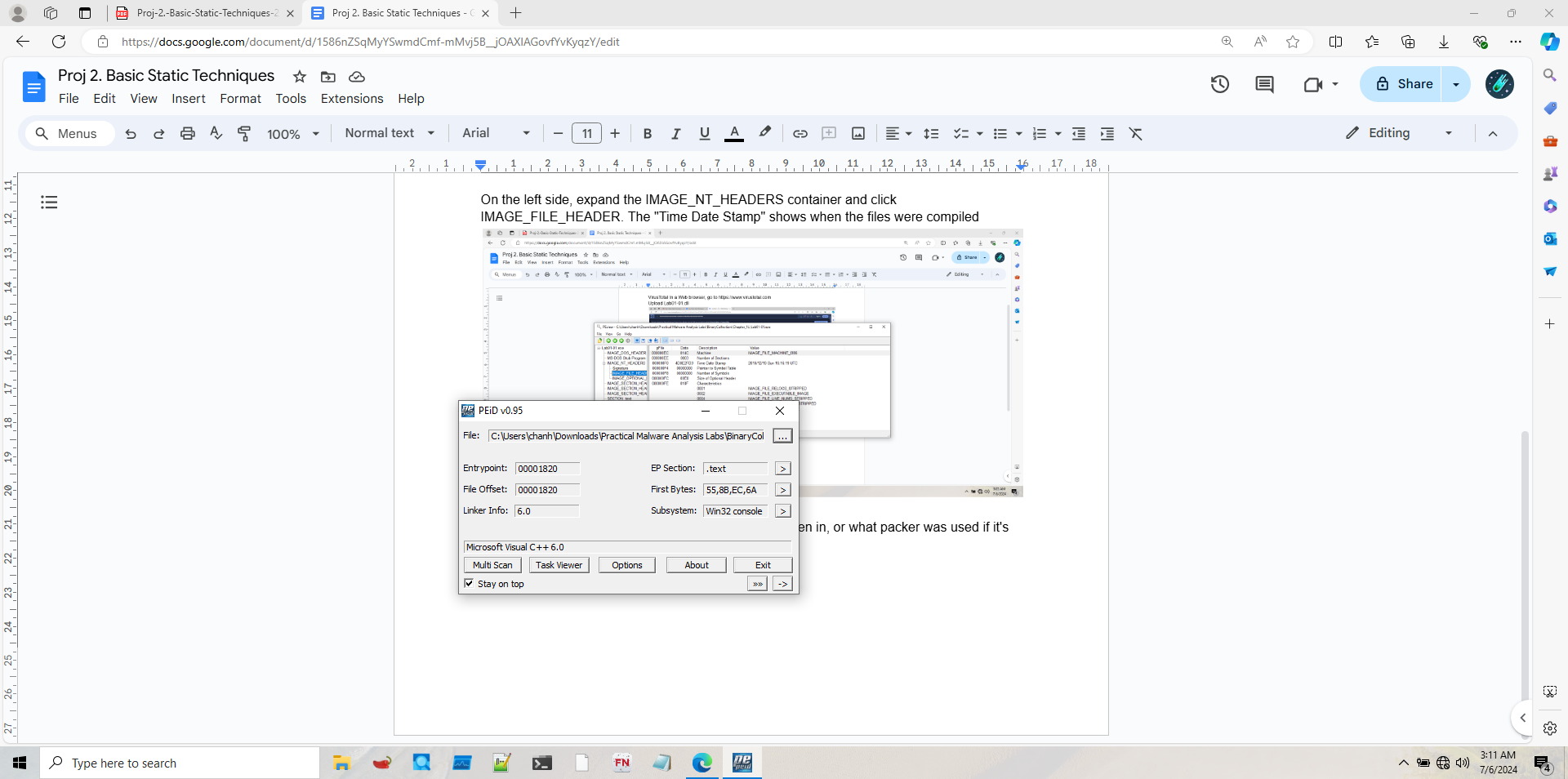


PEview shows the sections that make up a PE (Portable Executable) file

On the left side, expand the IMAGE\_NT\_HEADERS container and click IMAGE\_FILE\_HEADER. The "Time Date Stamp" shows when the files were compiled



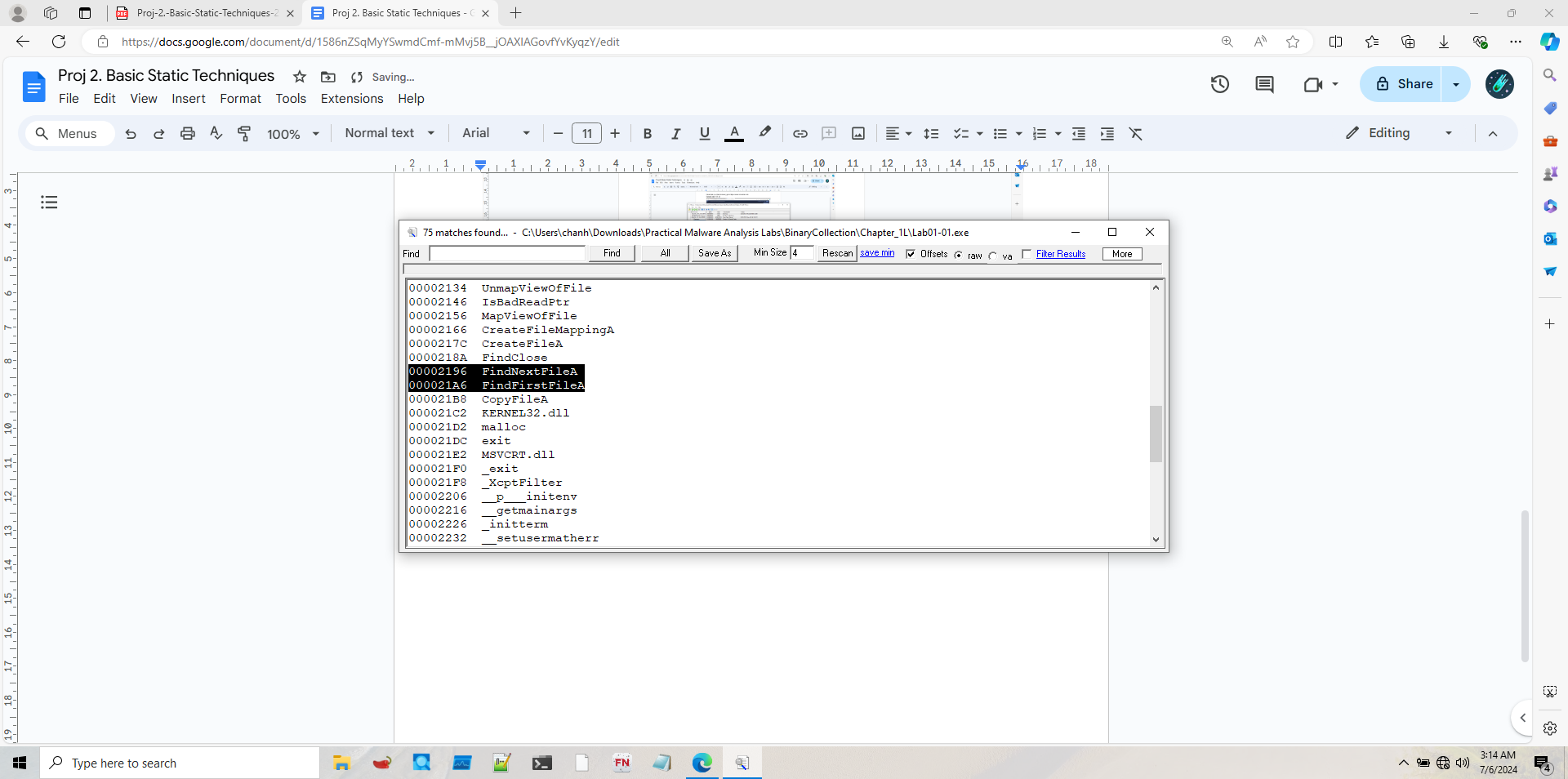
PEiD PEiD shows what language the sample was written in, or what packer was used if it's packe



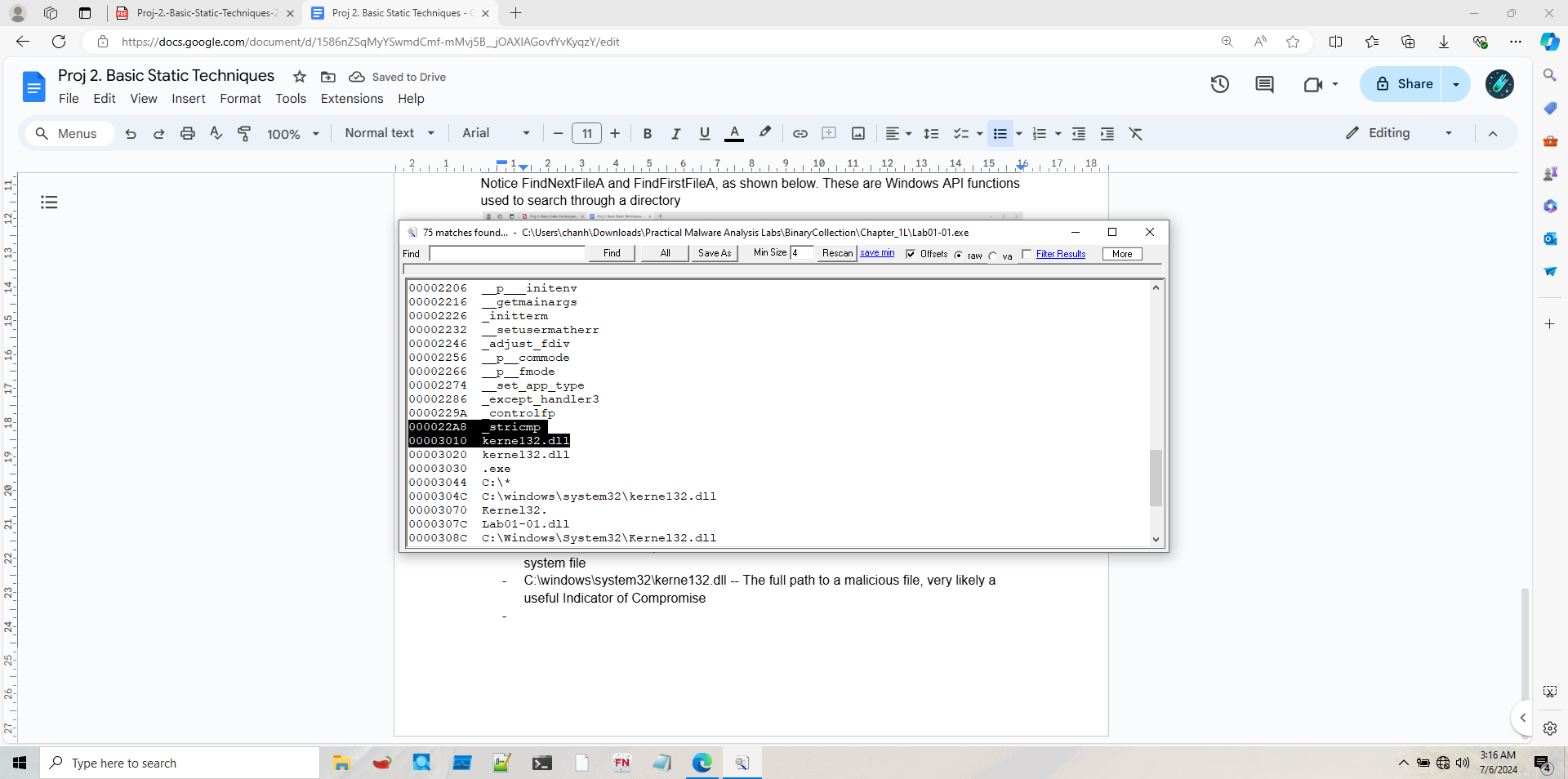
BinText

BinText is a handy tool to view strings, a very easy and powerful way to analyze a file

Notice FindNextFileA and FindFirstFileA, as shown below. These are Windows API functions used to search through a directory



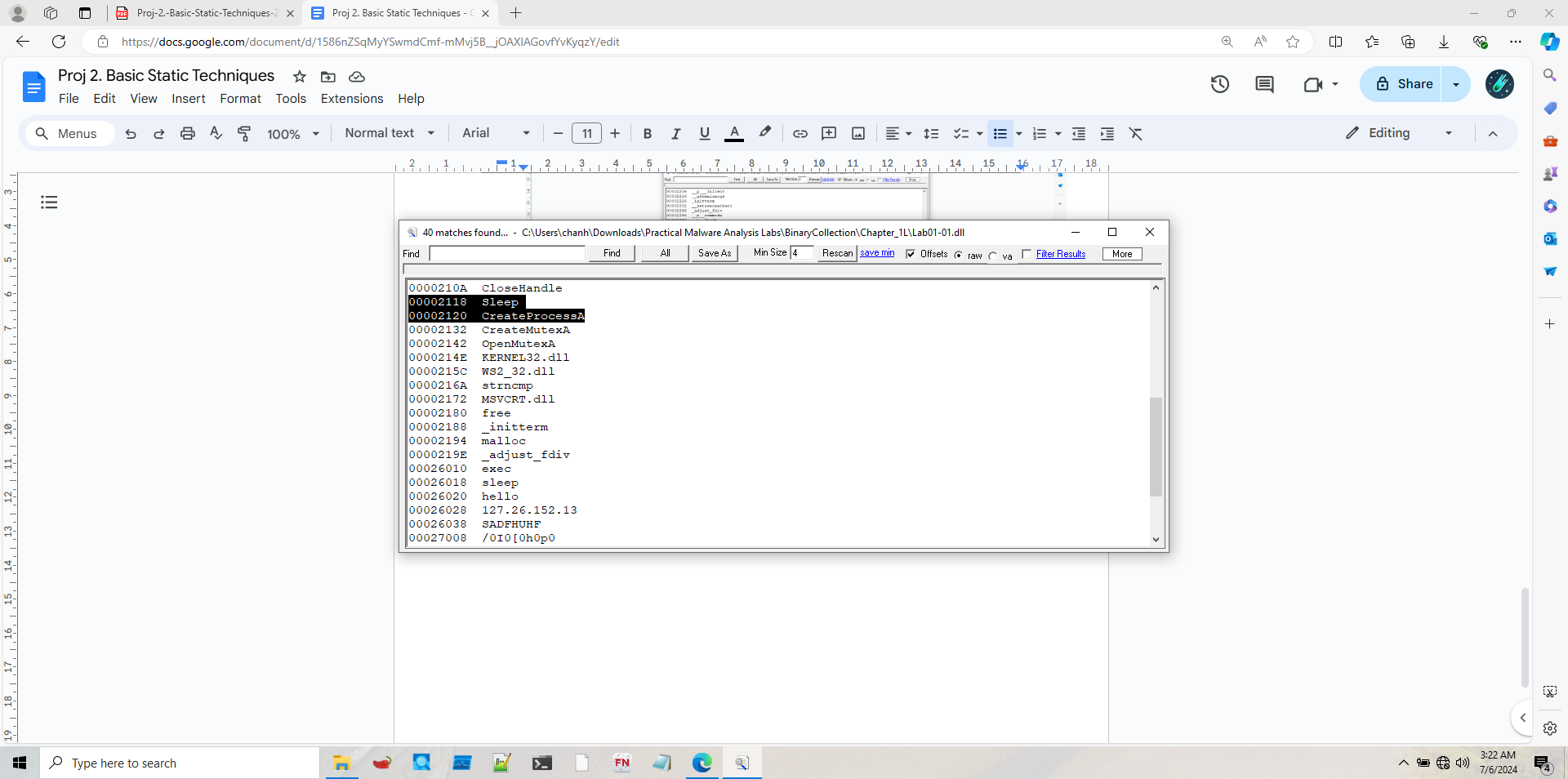
Scroll down and find these items, as shown below.

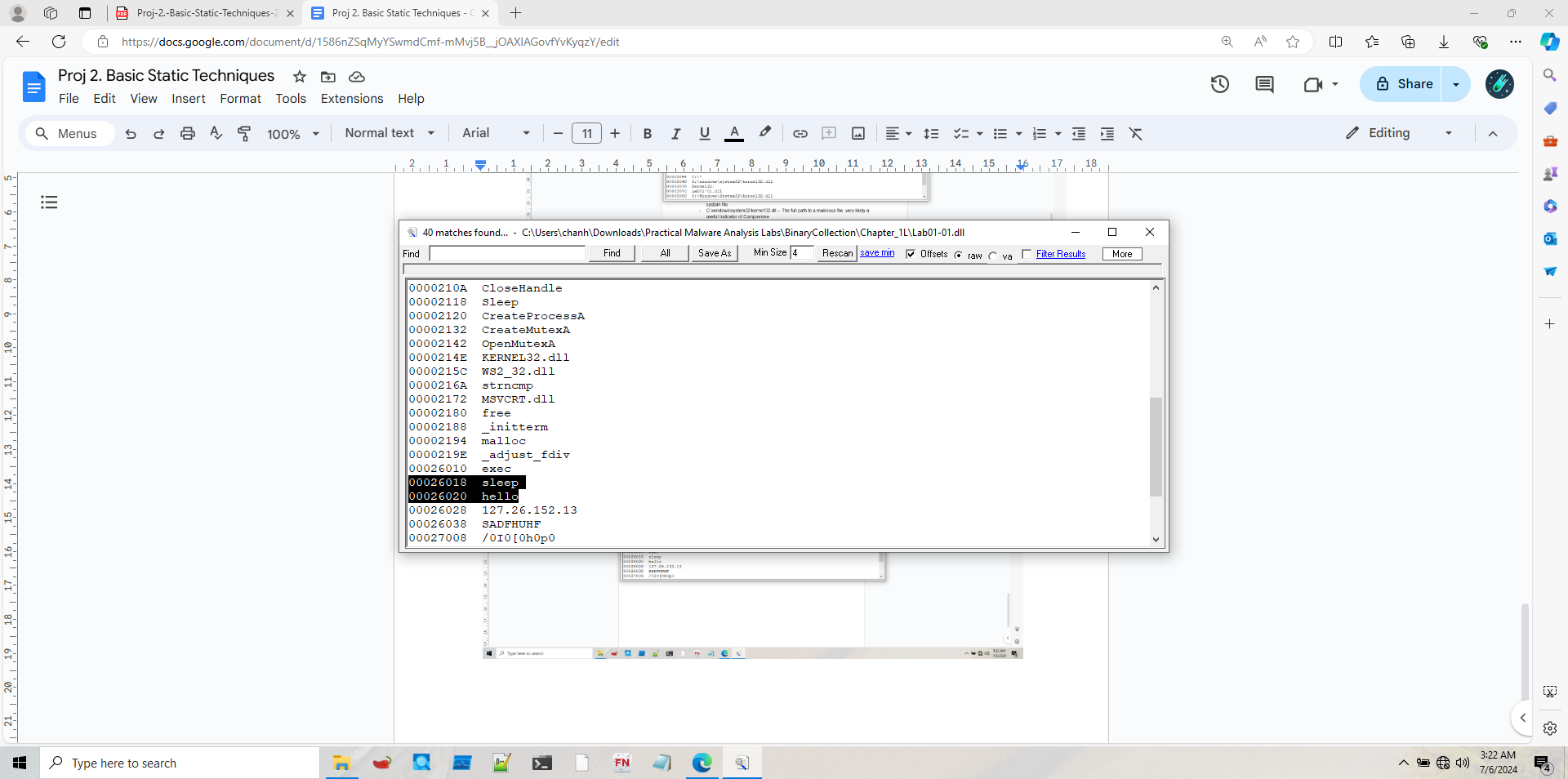
* \_stricmp -- Compares a string to a desired value
* kerne132.dll -- A deceptive filename to make the malware look like a Windows system file
* C:\windows\system32\kerne132.dll -- The full path to a malicious file, very likely a useful Indicator of Compromise
* 

In BinText, open the Lab01-01.dll file and click Go.

Notice these items, as shown below:

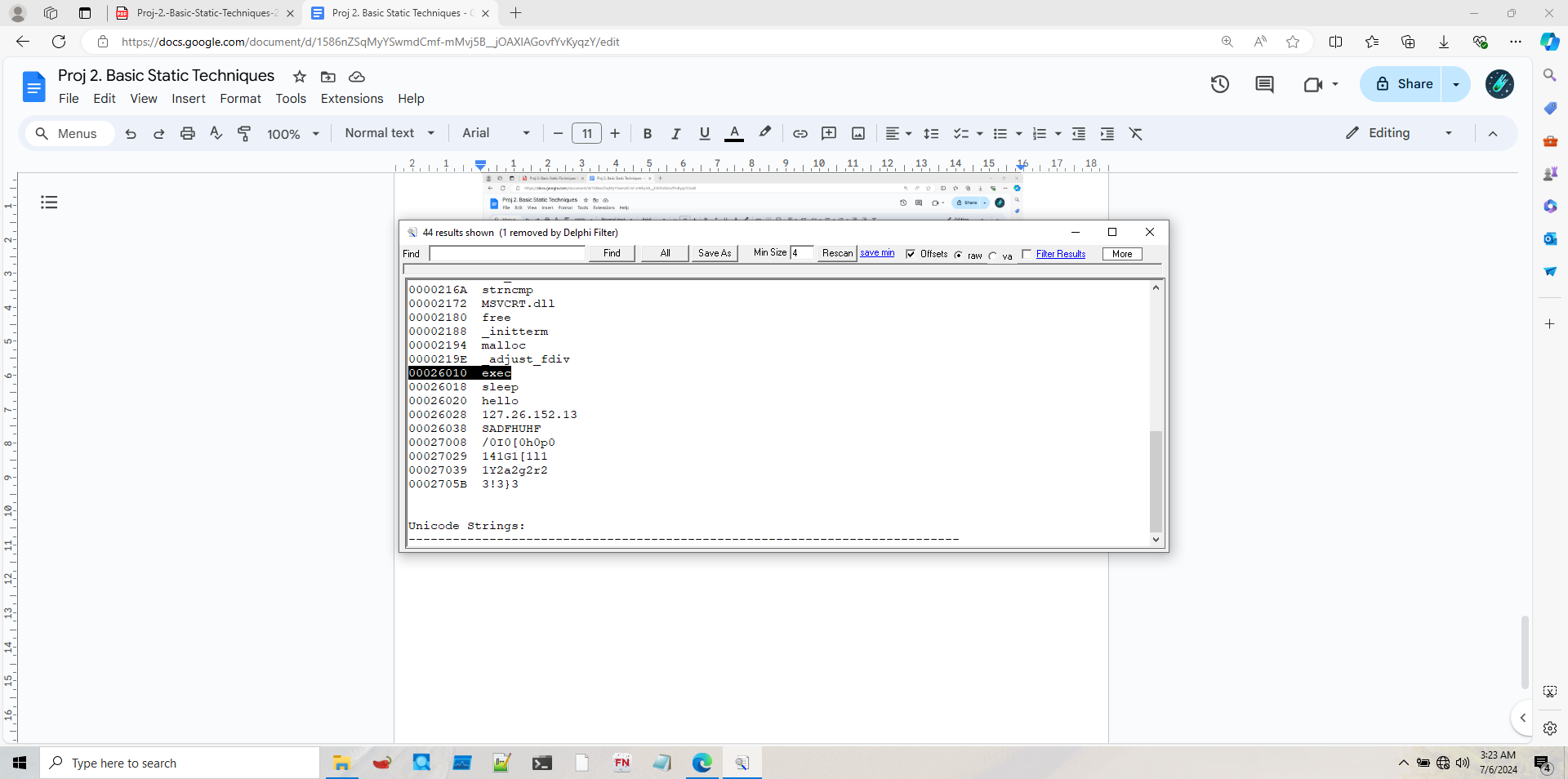
* Sleep -- Windows API function used to sleep
* CreateProcessA -- Windows API function used to launch a program
* sleep and hello -- Commands that can be sent over the network to tell the malware to sleep, and some function called "hello"





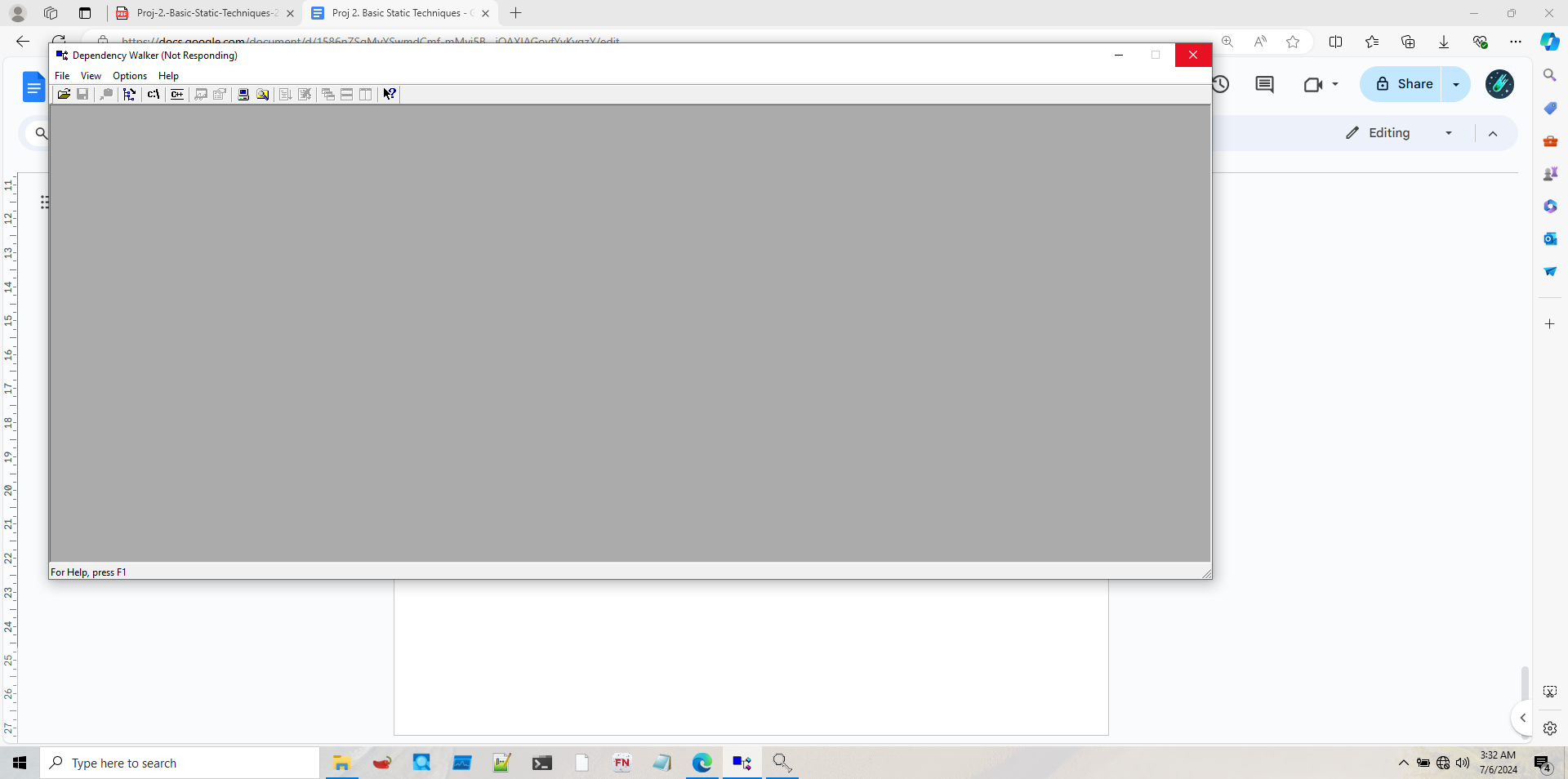
The command to launch a program is missing

Now you can see that the command to launch a program is exec, as shown below



Dependency Walker

Launch Dependency Walker. In Dependency Walker, click the opening folder icon and open the Lab01-01.exe file



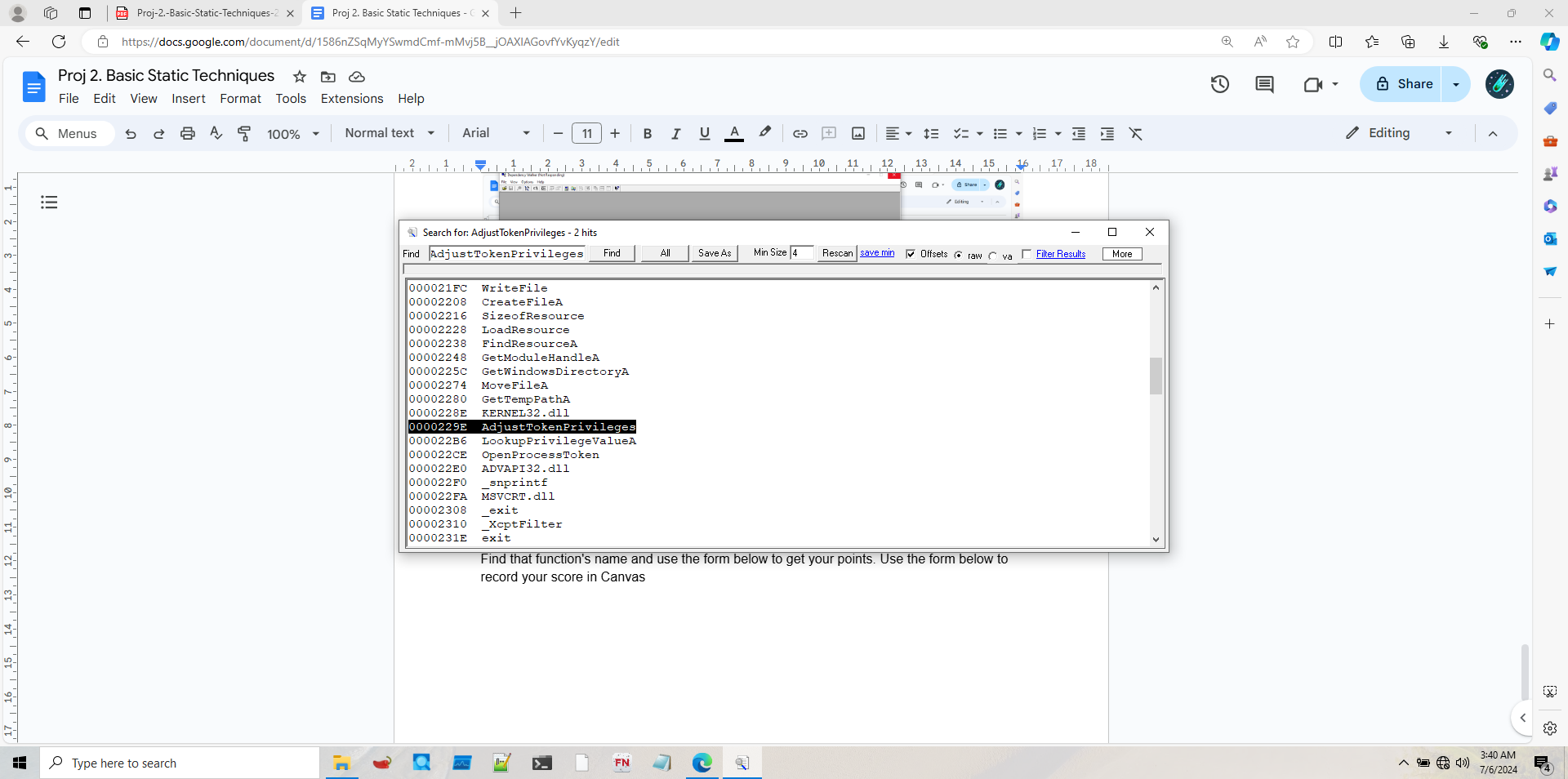
It so lagged so we move next

Extra

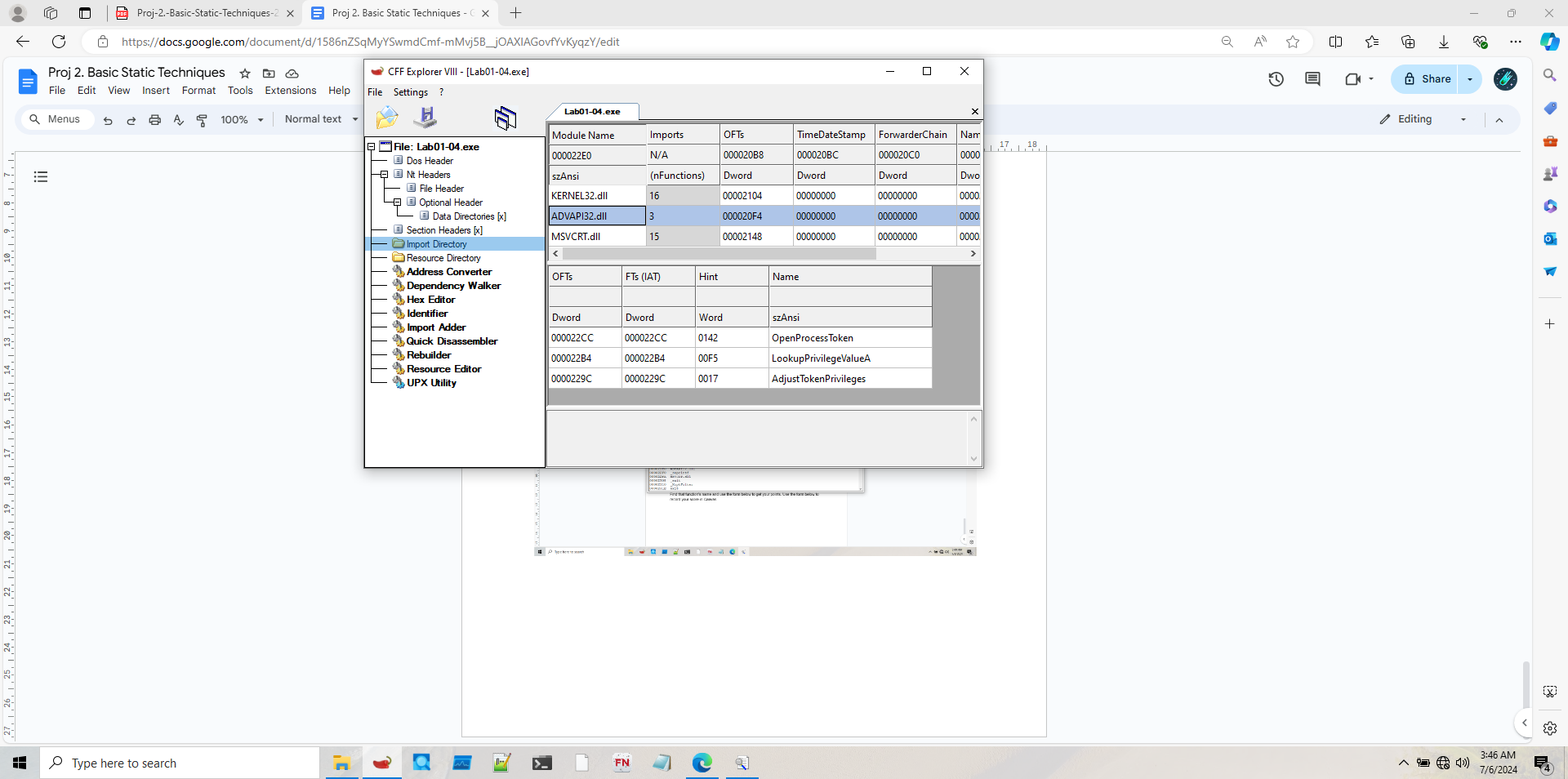
Find the Imported Function

Analyze the sample Lab01-04.exe It imports a function from WINTRUST.DLL

Find that function's name and use the form below to get your points. Use the form below to record your score in Canvas



Find the Imported Function (10 pts extra credit) Analyze the sample Lab01-04.exe It imports a function from WINTRUST.DLL



Time date stamp

