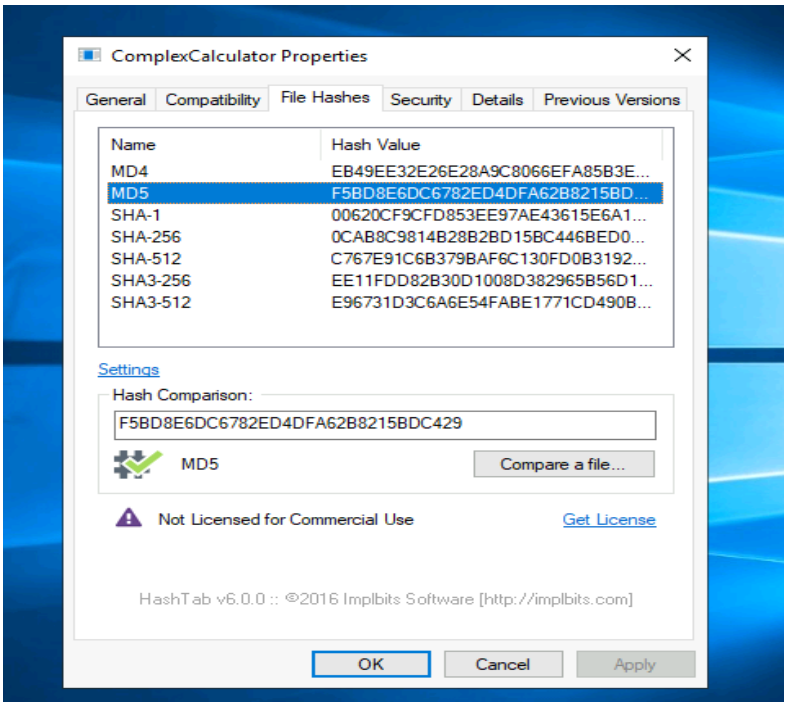
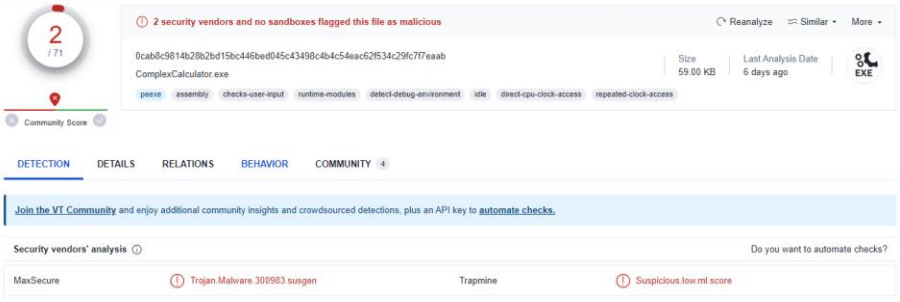
This is a small project to show basic malware analysis using common tools used to discover malicious software and files.

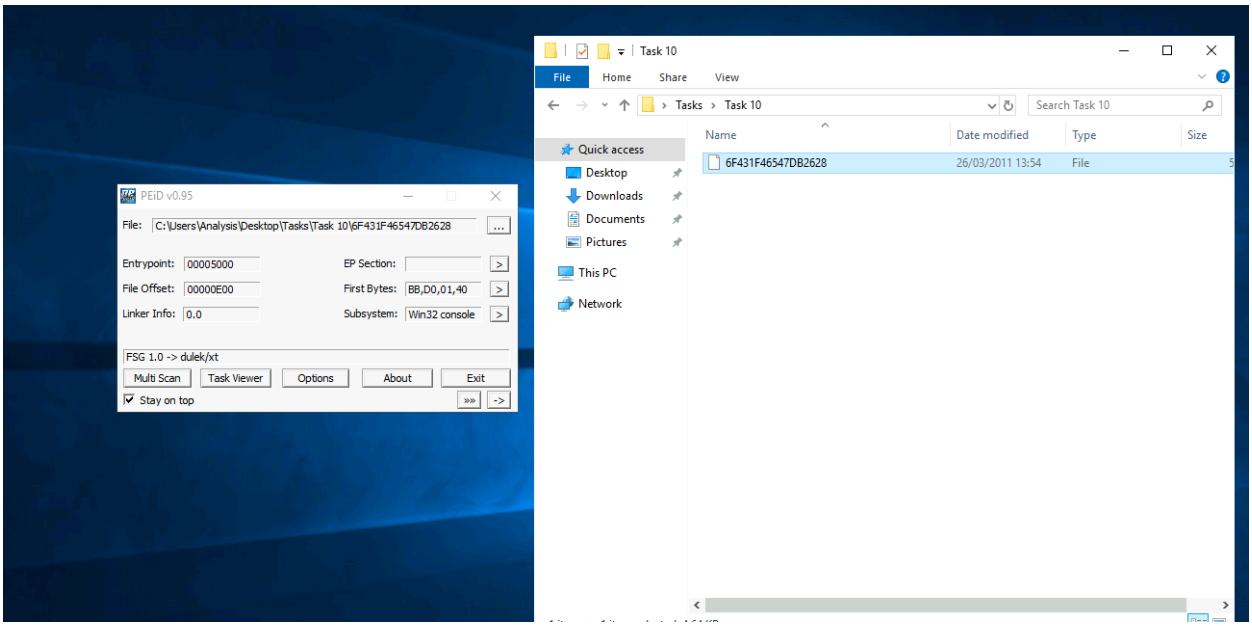
Using a tool called virustotal which can be found through a browser search, I was able to check the file hashes of executable files to determine malicious coding. The image below shows an example of finding the MD5 file hash.



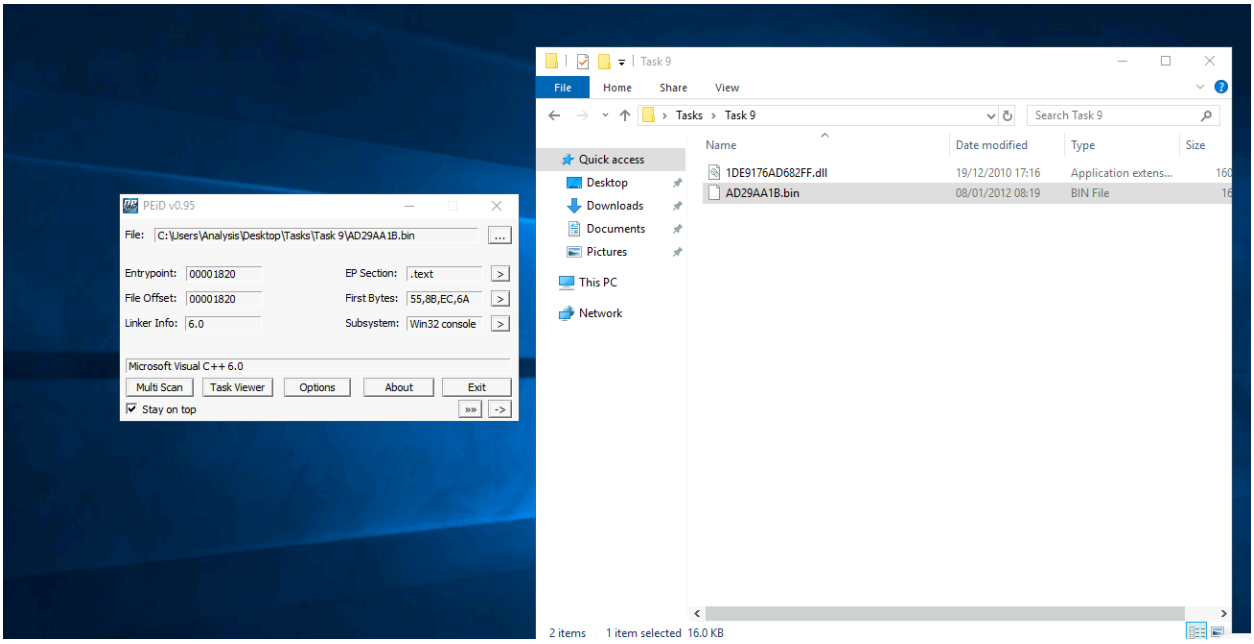
After finding the File Hash, it was then inputted in virustotal to identify if that hash has ever been reported as malicious. Sure enough, it was reported to have a trojan embedded into the file.



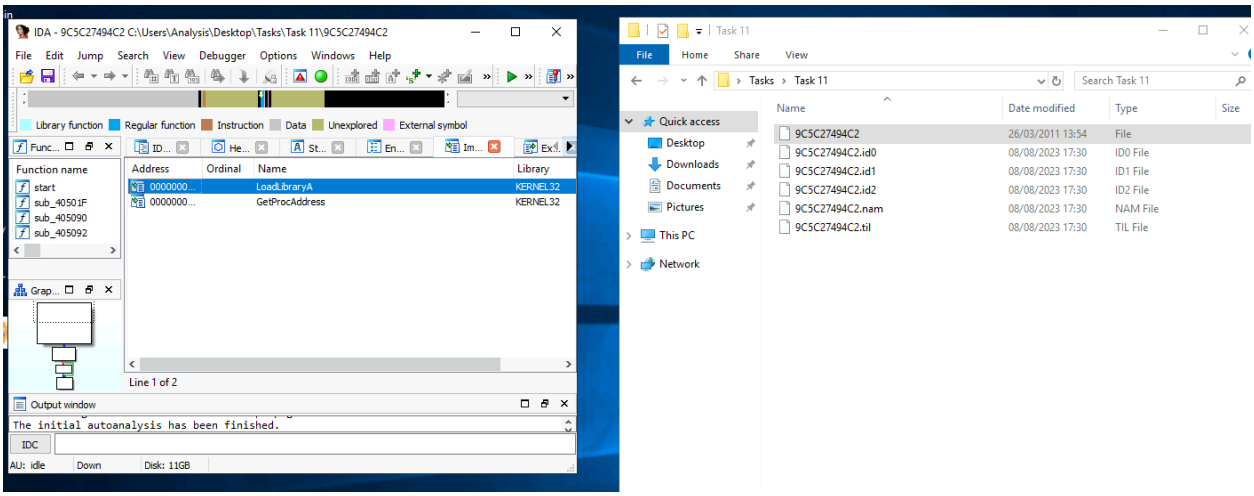
I had other files predownloaded into my virtual machine, and I wanted to check on their origins using peID. The image below shows that the file is from FSG 1.0.



I scanned another file using peID only to find that it came from Microsoft itself which means it is safe to use.



Finally, there was a file that checked out to have very little data inside of it as seen with IDA Freeware. The image below shows that during deobfuscation, it was found that it was imported only twice which is odd.



Although this is a small project, I learned a great deal from this hands-on experience. I intend to learn more about malware analysis and conduct more projects.