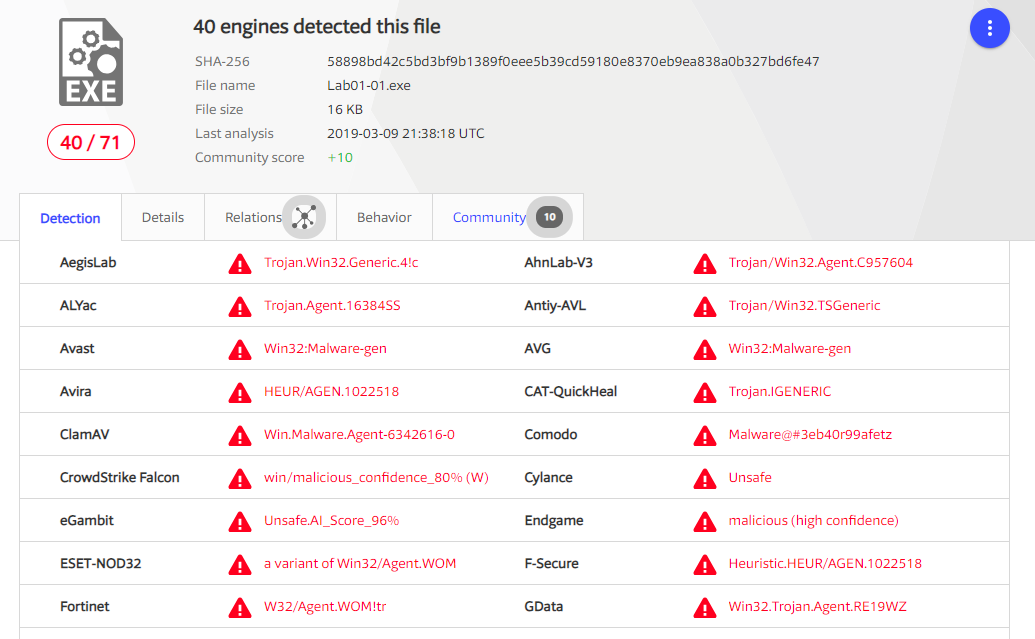
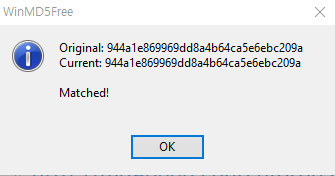
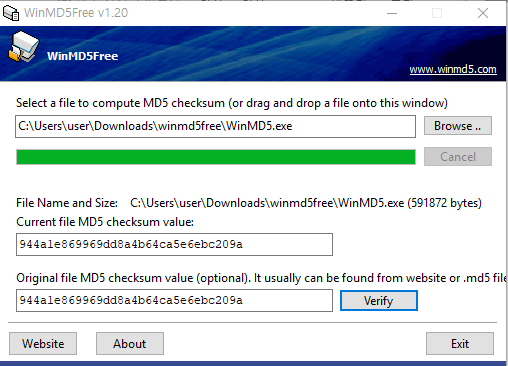
실습보고서1 2016111566 이나경

실습01) VirusTotal 사이트에 접속해서 간단한 프로그램 (노트 패드나 강의자료 악성코드)을 검증해보자



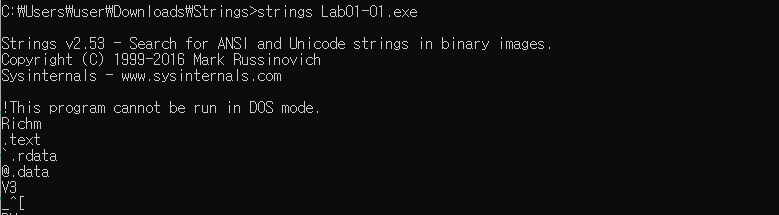
Lab01-01.exe를 스캐닝한 결과 71개 중 40개에서 악성코드가 탐지되었다.

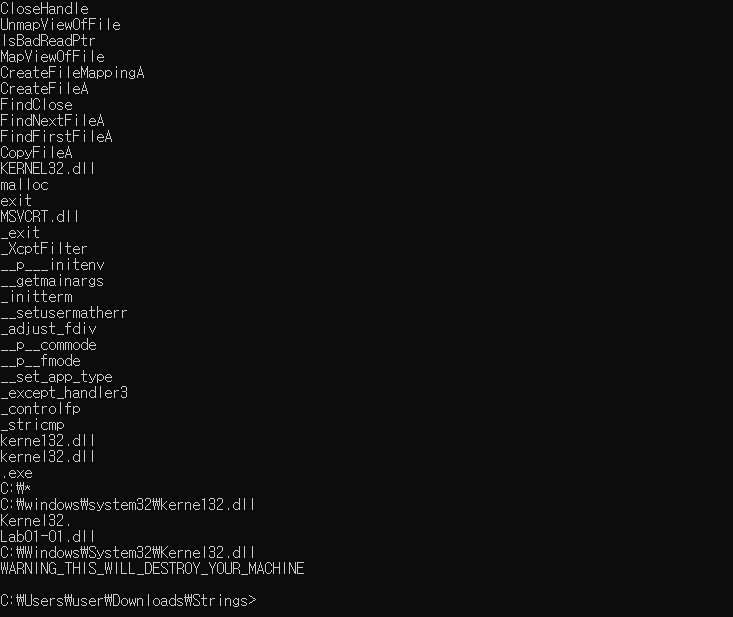
실습02) WinMD5Free SW를 다운받아 설치하고 검증해보자



해싱값이 일치하는 것을 확인하였다.

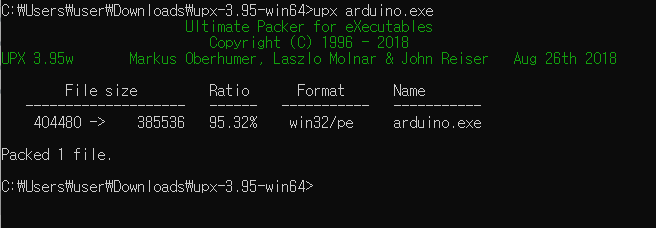
실습03) Strings를 다운받아 설치하고 악성코드가 어떤 결과로 나타나는지 실습해보자



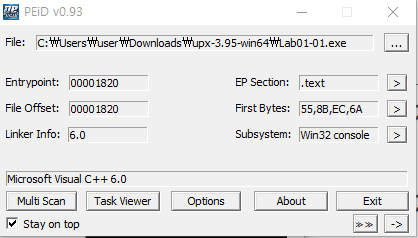


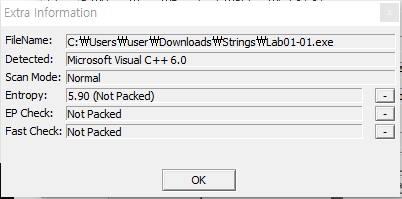
Strings로 Lab01-01.exe를 검색한 결과 CloseHandle, CreateFileA, CopyFileA 등의 함수가 임포트되어있는 것을 알 수 있었다.

실습04) UPX를 다운받아 정상프로그램을 패킹해봅니다. PEiD를 다운받아 설치하고 패킹 전후의 프로그램의 검증 과정에서 변화가 있는지 확인해봅니다.

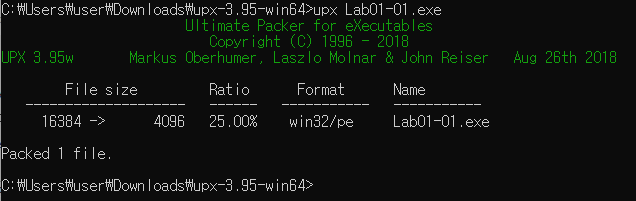


먼저 upx로 정상 프로그램인 아두이노 실행파일을 패킹해보았다.

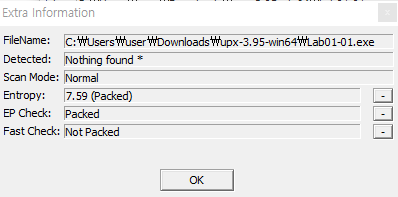
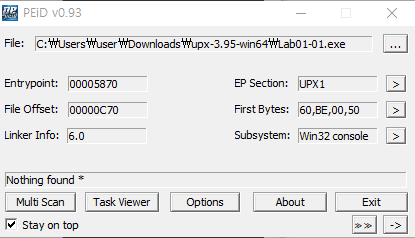




먼저 PEiD로 패킹 전의 Lab01-01.exe 파일을 탐지해보았다. Not Packed로 나오는 것을 확인하였다.

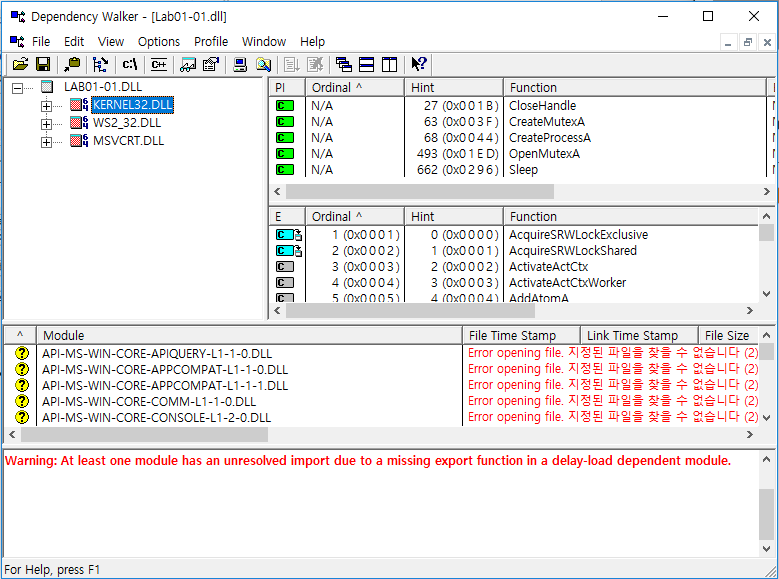


Upx로 Lab01-01.exe 파일을 패킹한 후 PEiD로 탐지한 결과

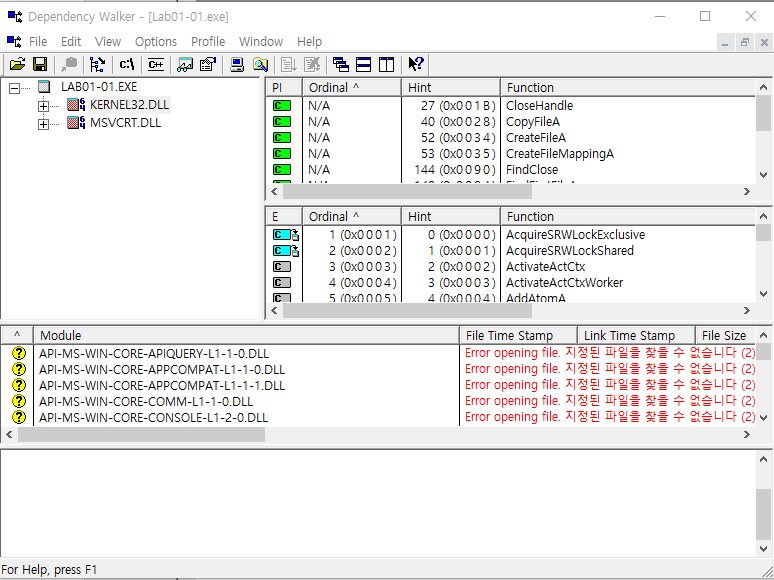


패킹된 것을 확인할 수 있었다.

실습05) Dependency Walker를 다운받아 설치하고 프로그램에 따라서 어떠한 특징을 보이는지 확인해봅니다

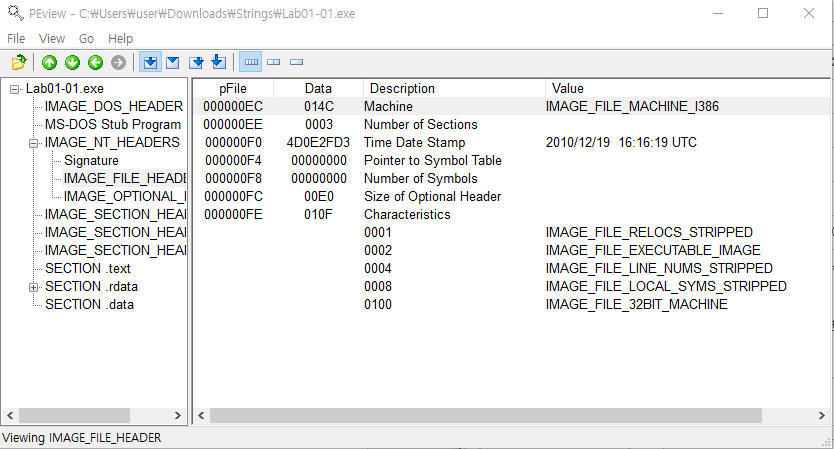


Lab01-01.dll을 탐지한 결과 CreateProcessA, OpenMutexA 등의 함수를 찾아볼 수 있었다.



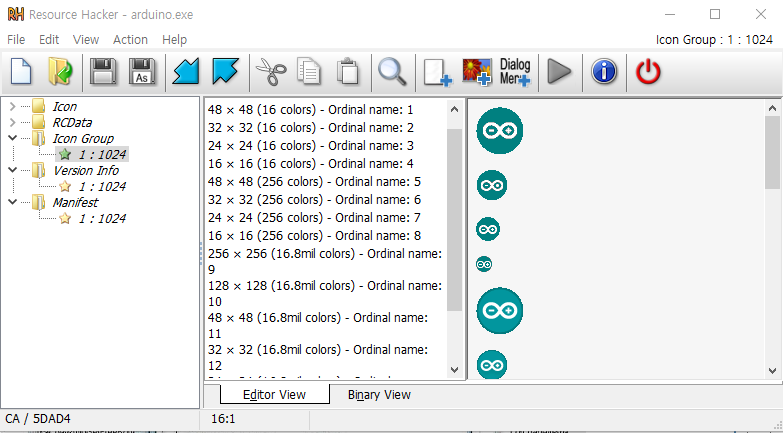
Lab01-01.exe을 탐지한 결과 CopyFileA, CreateFileA, FindFirstFileA 등의 함수를 찾아볼 수 있었다.

[PEview 실행화면]



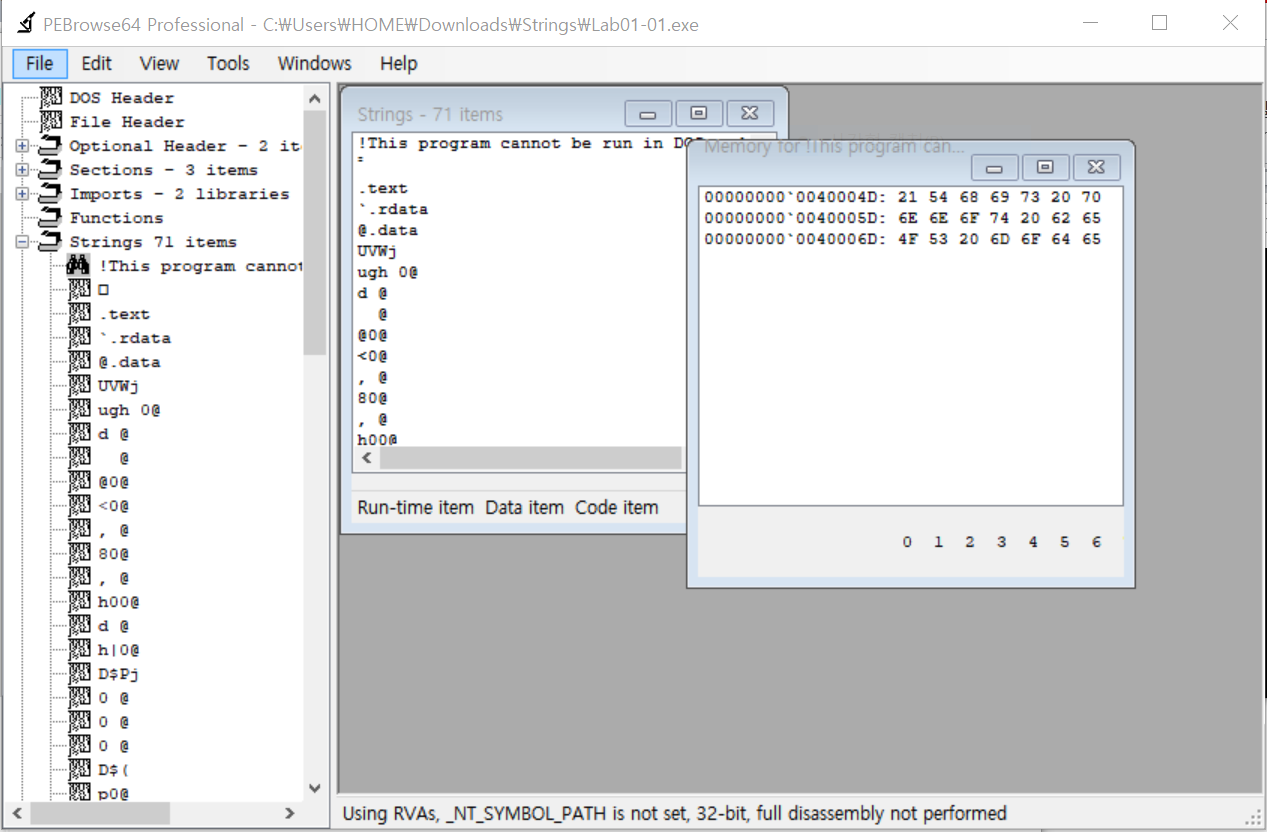
Lab01-01.exe파일의 PE파일을 점검하였다.

[ResourceHacker실행화면]



아두이노 실행파일을 탐지해보았다.

[PEBrowse(string부분)]



Lab01-01.exe파일의 Strings 부분을 점검하였다.