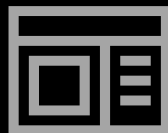


리버싱 이론



Made by Lamed



TOOLS :

Visual Studio 2019
X64dbg

Contents

Chapter 1 :

Chapter 2 :

Chapter 3 :

Chapter 4 :

Chapter 5 :

Chapter 6 :

Chapter 7 :

Chapter 7 :

Chapter 1

Episode 1 :

Episode 2 :

Episode 3 :

Episode 4 :

Episode 5 :

Episode 6 :

Episode 7 :

Episode 7 :

Chapter 1

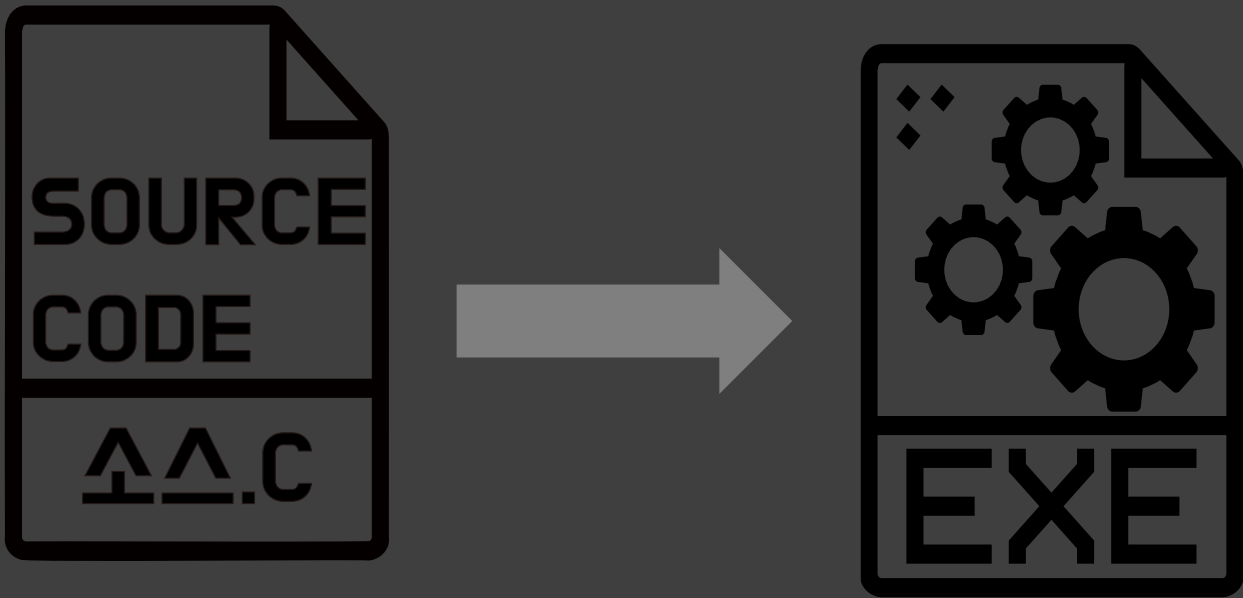
Episode 1

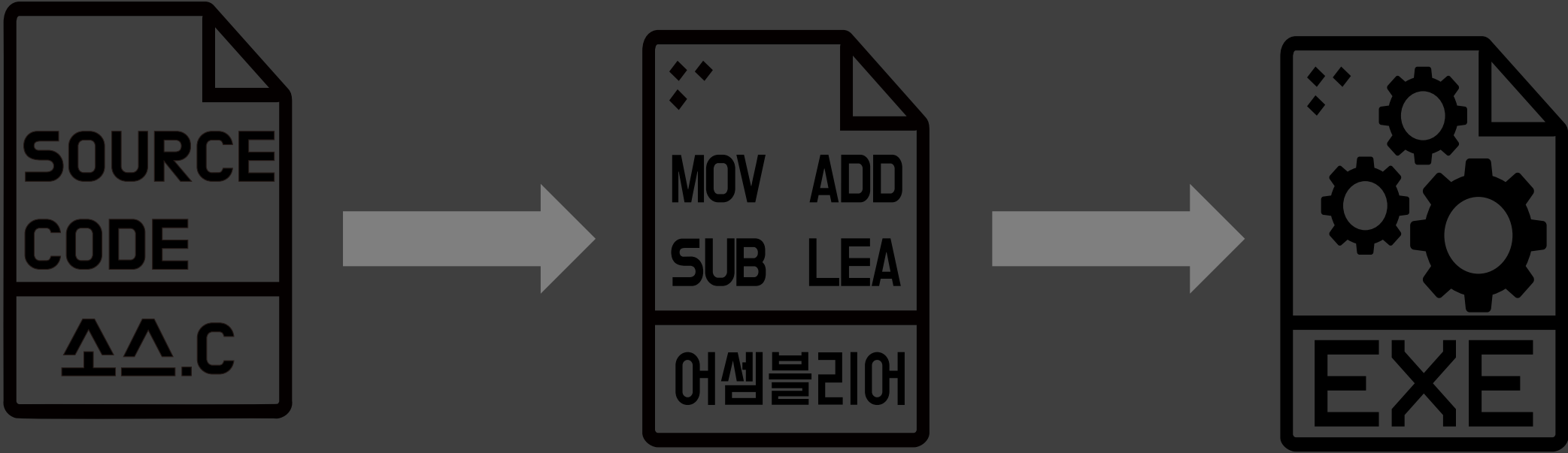
C언어

개념의 대한 새로운 활용



1. C언어

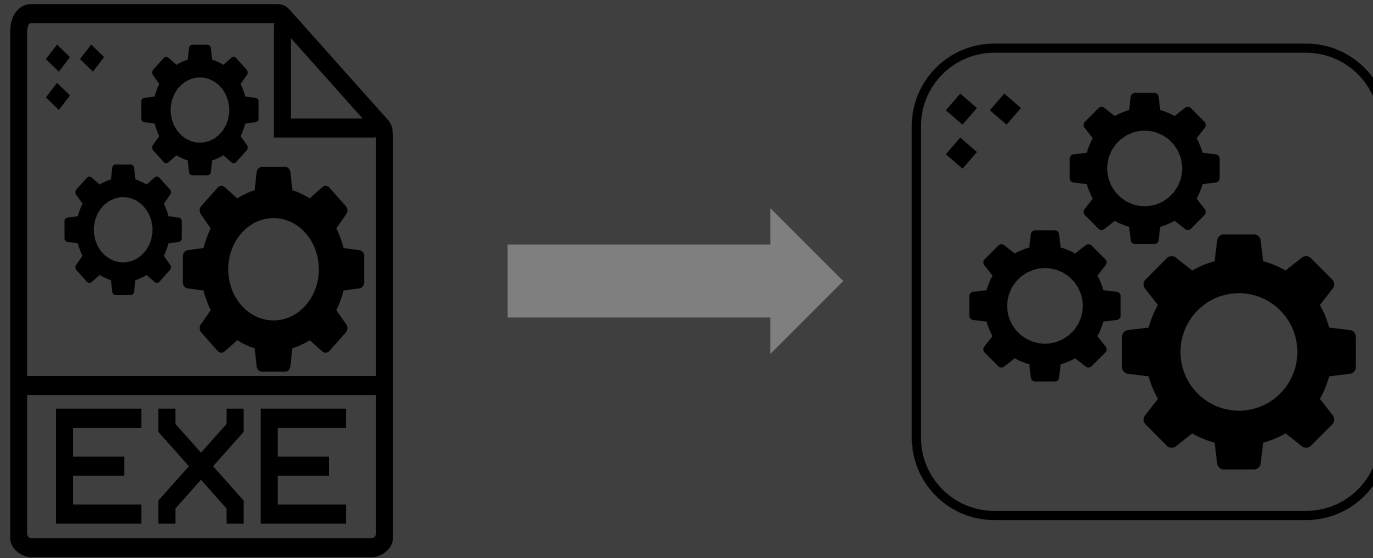




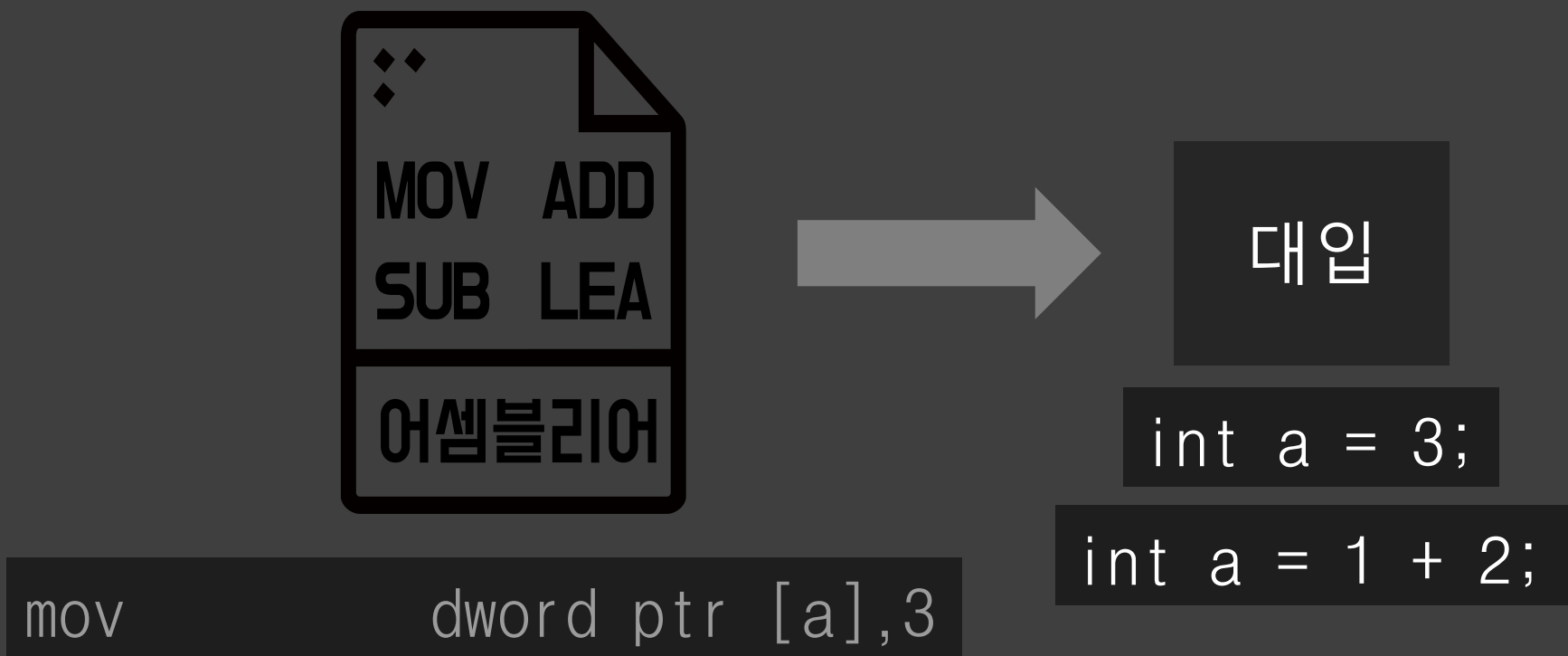
* 프로그램이 실행되면 프로세스가 된다.

1. C언어

라메드
Lamed



어셈블리어라는 기본언어를 보고 언어개발자들은 프로그래밍 개념을 만들었다.

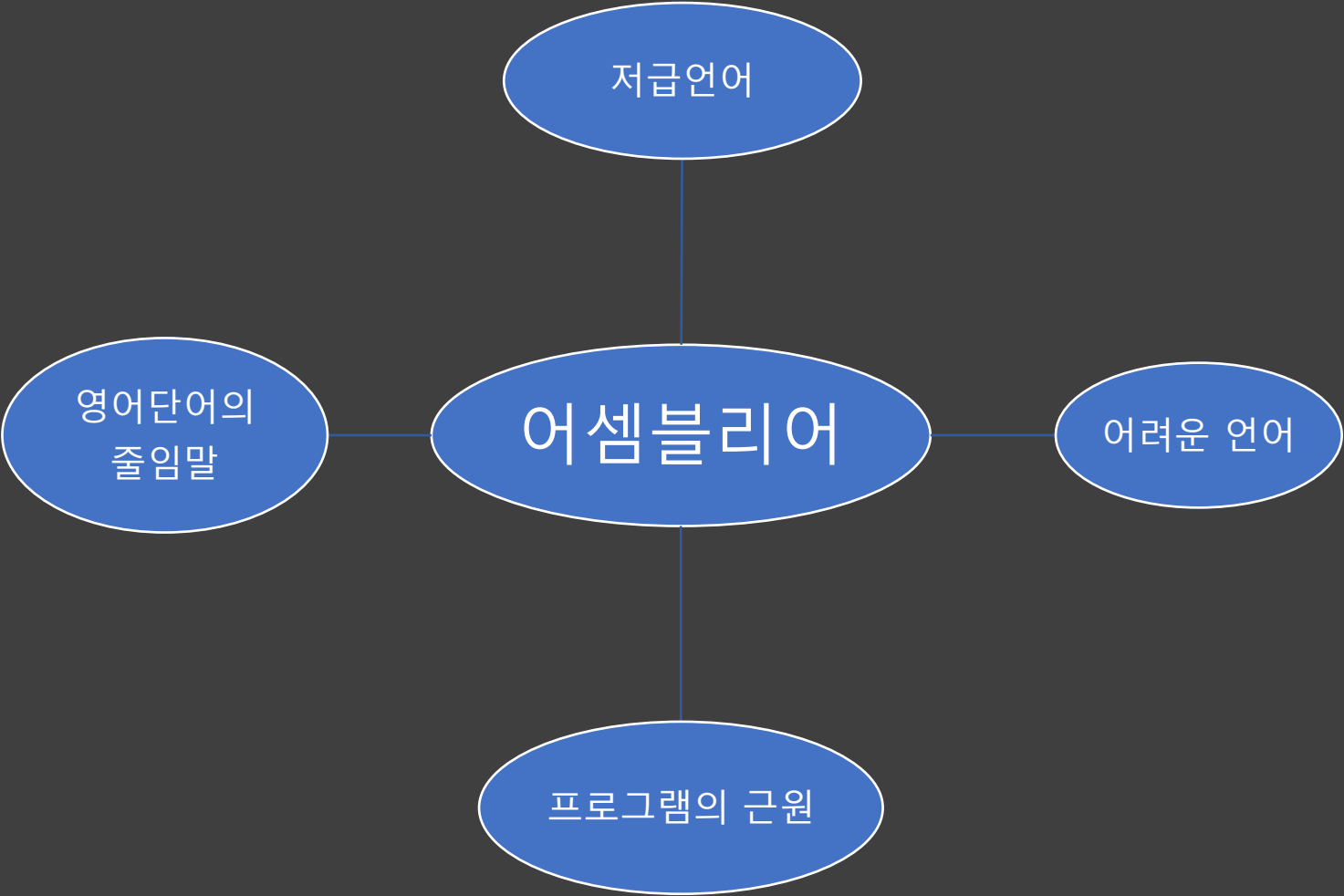


Chapter 1

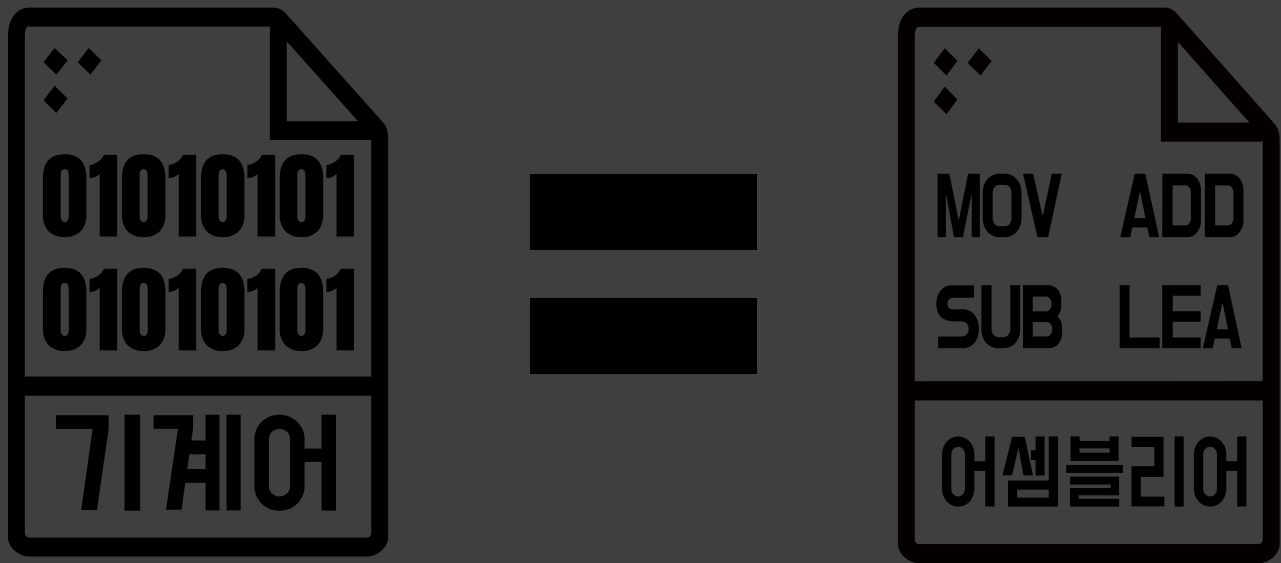
Episode 2

어셈블리어
프로그램의 원리

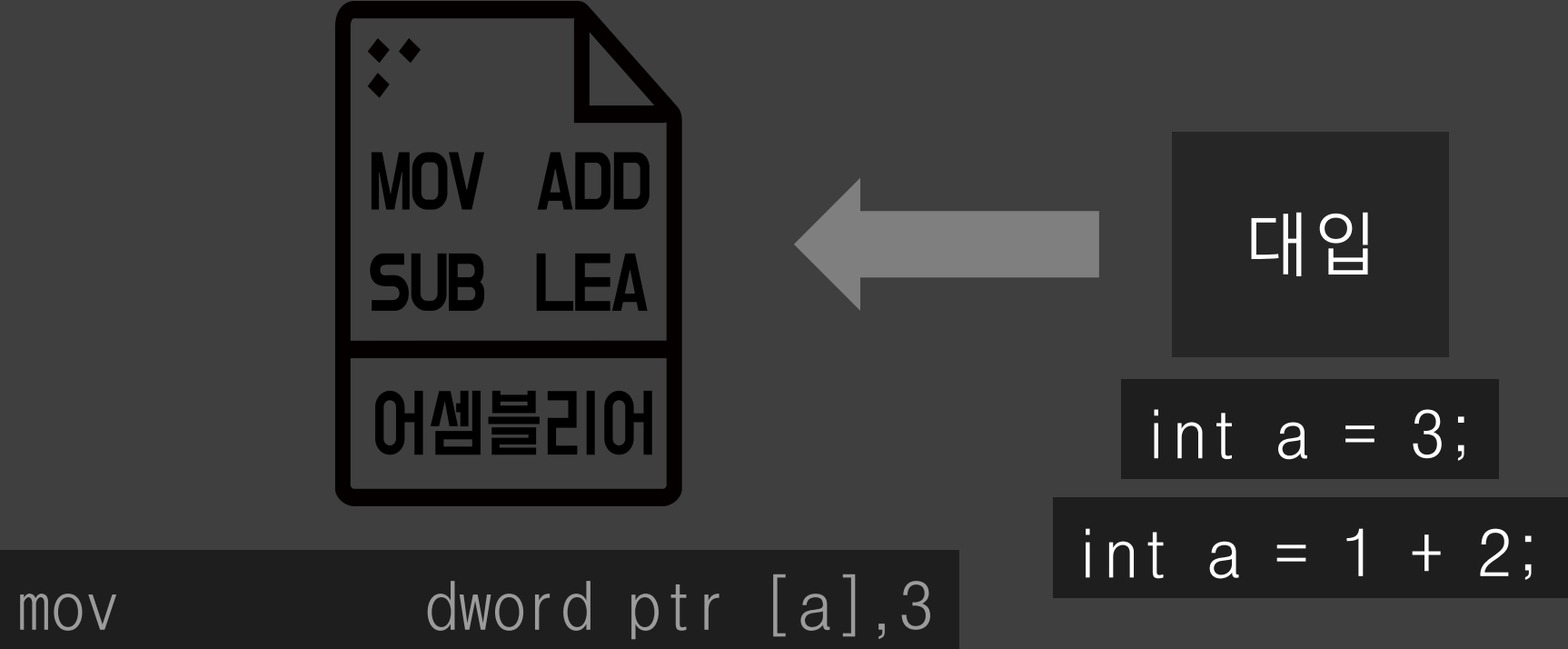
어셈블리어란 무엇일까?



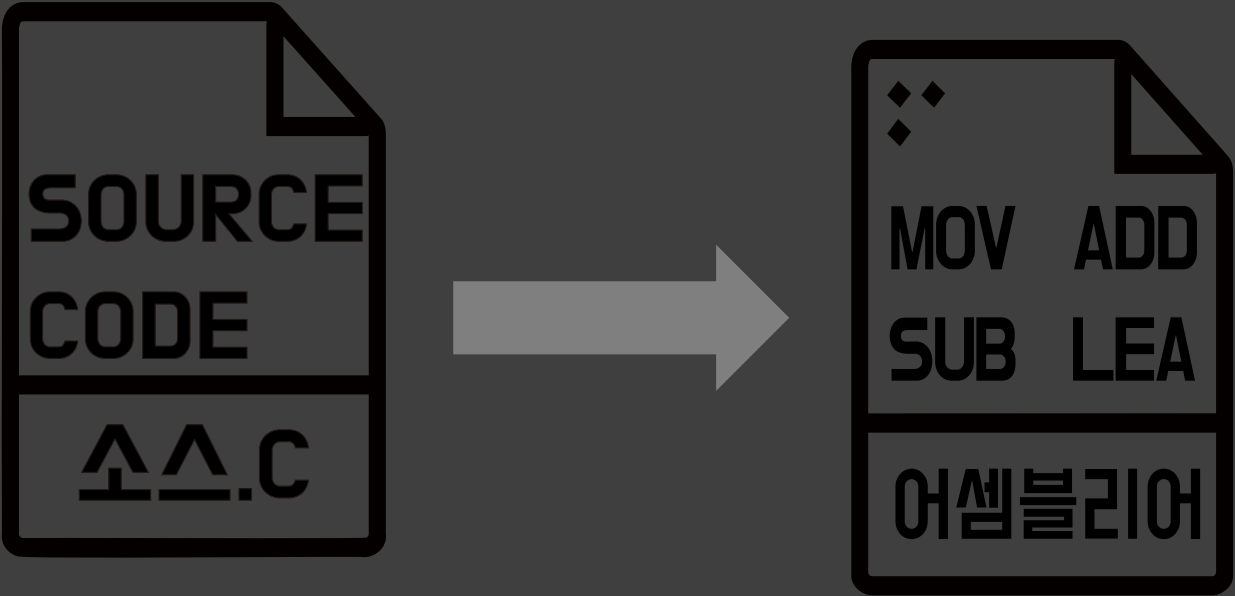
어셈블리어는 컴퓨터의 언어를 사람이 볼 수 있게 영어단어 줄임말을 사용했다.
어셈블리어 라는 언어는 기계어와 1대1 즉 기계어(01)을 다른 형태로 보여준 것이다.
어셈블리어는 단순하지만 개념들이 일상적이지 않아 어렵다



어셈블리어라는 기본언어를 보고 언어개발자들은 프로그래밍 개념을 만들었다.
그럼 어셈블리어에서 프로그래밍 개념을 생각했다면 역으로 공부 할 수 있지 않을까?



C언어는 프로그래밍의 기초라고 불리고 어셈블리어로 변환하는 언어이기 때문이다.



Chapter 1

Episode 3

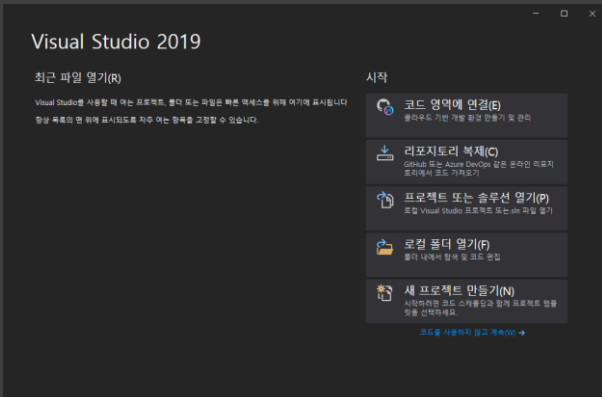
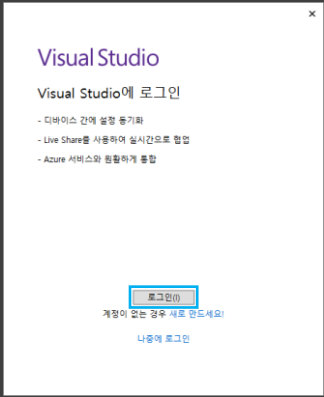
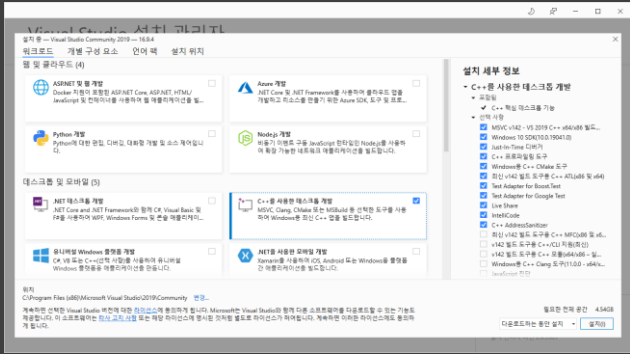
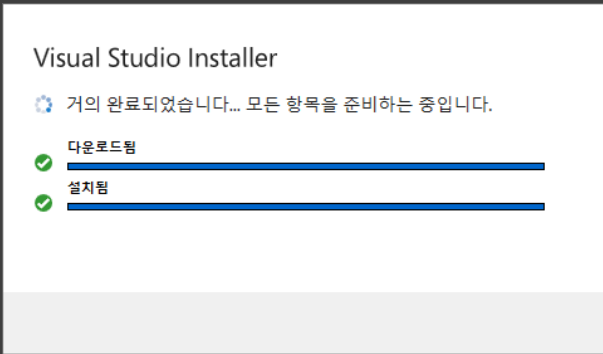
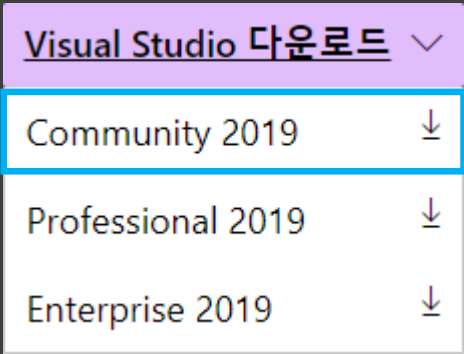
도구들

우리는 도구를 사용한다

3. 도구들

<https://visualstudio.microsoft.com/ko/vs/> ← 다운로드 주소

VS를 사용한 이유는 간단하다.(많이 사용한다.)
많이 사용하기 때문에 많은 프로그램이 VS로 만들어 진다.



<http://sourceforge.net/projects/x64dbg/files/snapshots> ← 다운로드 주소


디버거는 버그를 잡는 도구다.

디버거는 어셈블리어와 디버깅 기능을 통해 프로그램의 버그를 잡는 목적의 도구다.

하지만 어셈블리어와 디버깅 기능으로 프로그램을 분석할 수 있다.

SourceForge

Home / Browse / Security & Utilities / Security / x64dbg / Files

 **x64dbg**
An open-source x64/x32 debugger for windows.
Brought to you by: mrexodia

Summary Files Reviews Support Source

Download Latest Version
snapshot_2021-06-14_16-37.zip (33.1 MB) [Get Updates](#)

Home / snapshots

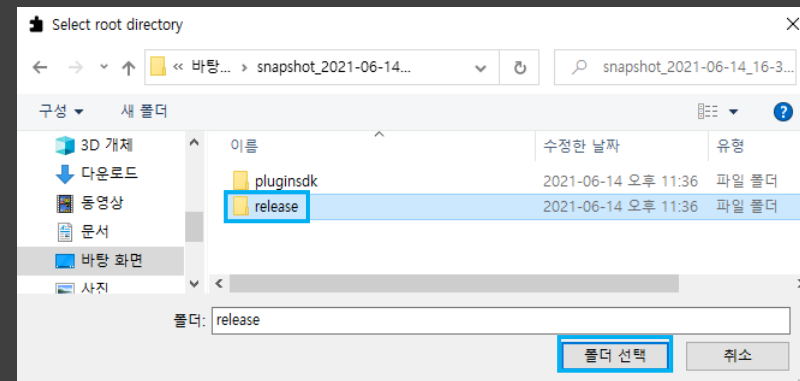
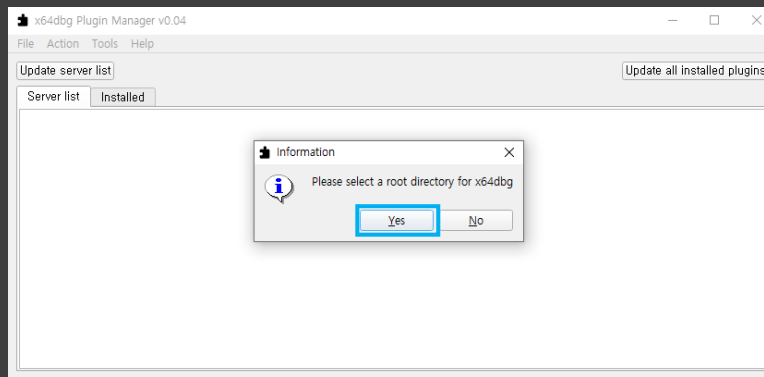
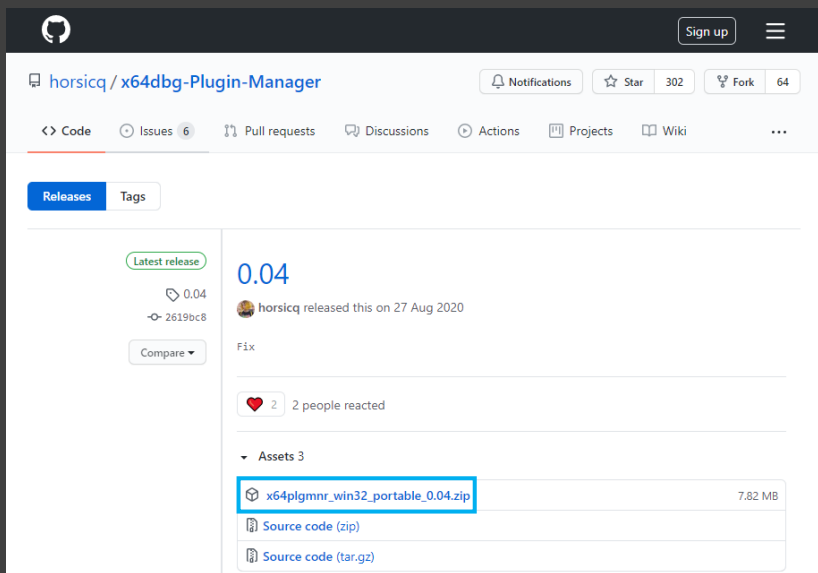
| Name | Modified | Size | Downloads / Week |
|---|------------|---------|------------------|
| Parent folder | | | |
| snapshot_2021-06-14_16-37.zip | 2021-06-14 | 33.1 MB | 4,883 |
| snapshot_2021-06-14_16-37-pdb.zip | 2021-06-14 | 21.6 MB | 62 |

<https://github.com/horsicq/x64dbg-Plugin-Manager/releases> ← 다운로드 주소

사람들은 디버거의 기능을 많이 만들었다.

게임의 모드들처럼 여러 기능들이 있다.

자기가 원하는 플로그인을 설치하면 된다.

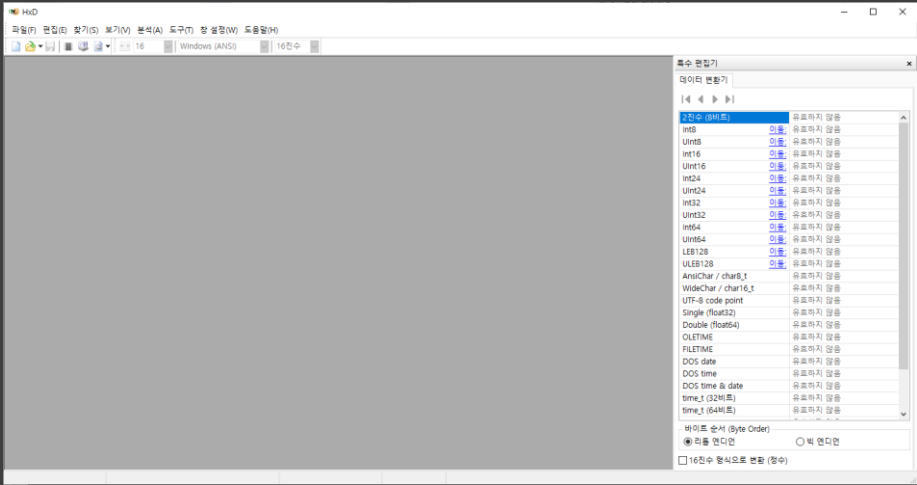
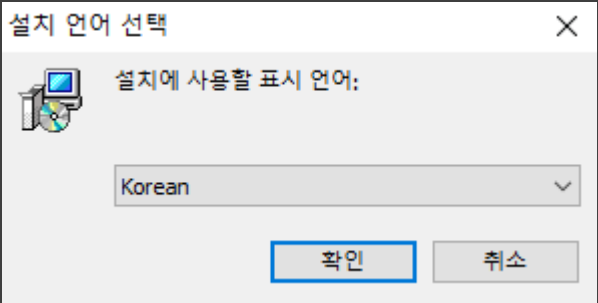




3. 도구들

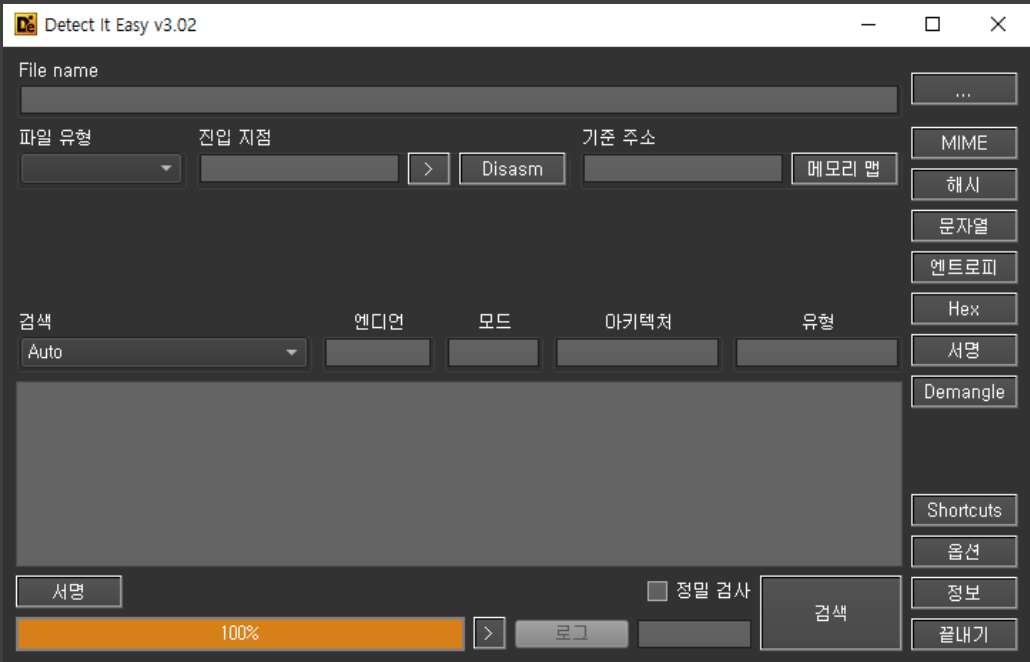
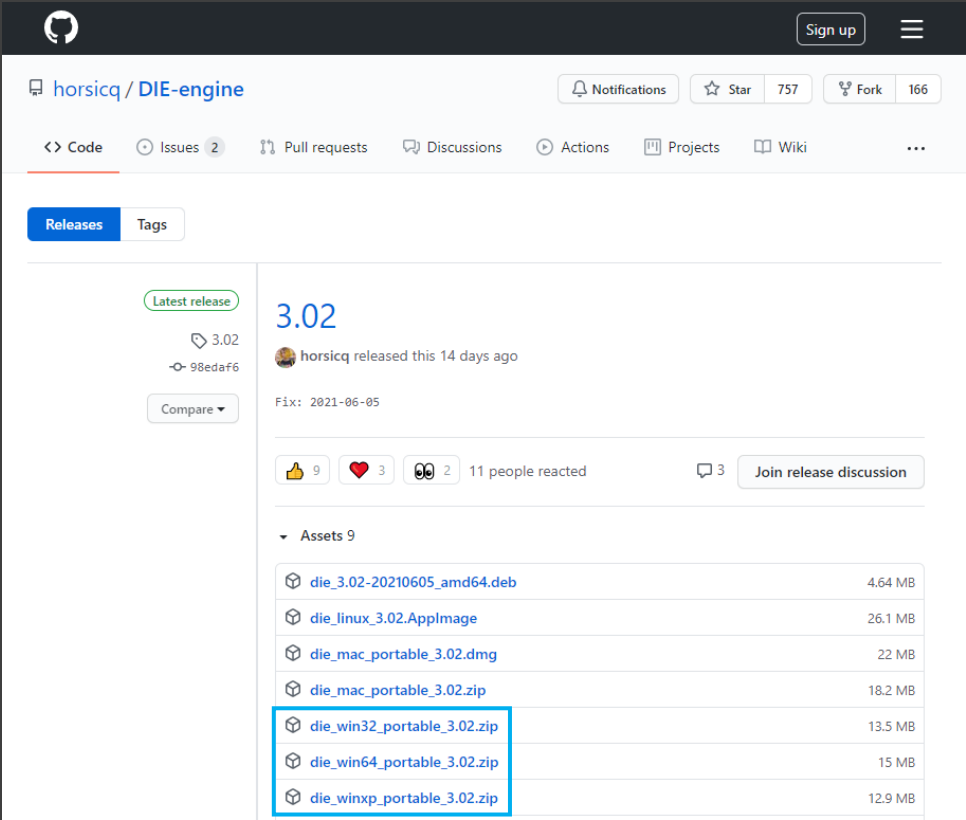
<https://mh-nexus.de/en/downloads.php?product=HxD20> ← 다운로드 주소

Hex editor(16진수 에디터) : 16진수의세계를 보여주는 눈이 될 도구입니다.



<https://github.com/horsicq/DIE-engine/releases> ← 다운로드 주소

프로그램이 어떤 도구로 개발되었는가 그런 흔적을 조사해주는 도구



프로그램은 설정을 갖고 있다.
설정값을 보여주고 쉽게 수정해주는 도구이다.

[– Explorer Suite \(Multi-Platform Version, Recommended\)](#)
SHA1: 89CAB44D4956210570AB3123FBBF13B2B7D870B91
SHA256:
94F4348EC573B05990B1E19542986E46DC30A87870739F5D5430B60072D5144D

[– CFF Explorer \(x86 Version, stand-alone, Zip Archive\)](#)
SHA1: 7A287CD97BD9287C020C98C3496E284D04F5382D
SHA256:
8E72BCB9C6E83F188F4A259AD039ED3CC37CDF2C3EA12B00F0DF8D8B67E96D96

[– CFF Explorer Extensions Repository](#)

CFF Explorer was designed to make PE editing as easy as possible, but without losing sight on the portable executable's internal structure. This application includes a series of tools which might help not only reverse engineers but also programmers. It offers a multi-file environment and a switchable interface.

September 29, 2019

- Video: Using Cerbero for CTFs
September 1, 2019
- Video: Yet another PDF/XDP Malware
August 5, 2019

RECENT COMMENTS

- Erik Pistelli on Time Travel: Running Python 3.7 on XP
- Adamski on Time Travel: Running Python 3.7 on XP
- Erik Pistelli on Time Travel: Running Python 3.7 on XP
- Maurice on Time Travel: Running Python 3.7 on XP
- Erik Pistelli on Time Travel: Running Python 3.7 on XP

ARCHIVES

