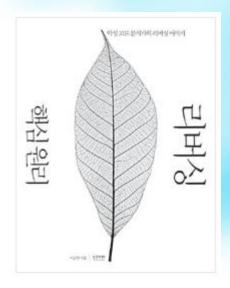


# 리버싱 - 핵심 원리 -





한양대학교 컴퓨터공학부 2014년 1학기 임을규

### 리버싱 스토리





- 리버스 엔지니어링
  - Reverse Engineering (RE) 또는 역공학
  - 물건, 기계 장치, 시스템 등의 구조, 기능, 동작 등을 분석하여 원리를 이해하고, 단점은 보완하고, 새로운 아이디어를 추가하는 작업
- Reverse Code Engineering (RCE)
  - SW 분야의 Reverse Engineering
  - '리버싱'이라고도 표현
  - 정적 분석 vs. 동적 분석

## 정적 분석 vs. 동적 분석





- 정적 분석
  - 파일을 실행하지 않고, 겉모습을 관찰하여 분석
  - 파일의 종류, 크기, 헤더 정보, import/export API, 내부 문자열, 실행 압축 여부, 등록 정보, 디버깅 정보, ...
  - 디스어셈블러(disassembler)를 이용하여 코드 분석
- 동적 분석
  - 파일을 직접 실행시켜 행위를 분석
  - 디버깅을 통행 코드 흐름과 메모리 상태 분석
- 일반적인 분석 방법
  - 정적 분석을 통해 정보 수집
  - 동적 분석을 통해 코드 등 분석

2014

## 패치와 크랙





- 패치
  - 프로그램의 파일 혹은 실행 중인 프로세스 메모리의 내용을 변경하는 작업
  - •예: Windows 업데이트
- 크랙
  - 패치와 같은 개념
  - 특별히 그 의도가 비합법적이고 비도덕적인 경우
  - 저작권을 침해하는 행위에 주로 사용됨

2014

# 리버싱 준비물





- 목표
  - 자신만의 분명한 이유
- 열정
  - 목표를 향해 끈기 있게 나아갈 수 있게 해주는 힘
  - 지겨움/좌절 극복
- 구글/네이버

2014

# 기타





- 리버싱 방해물
  - 과욕
  - 조급함
- 리버싱의 묘미
  - Assembly 언어 분석
  - 실행 파일을 통하여 프로그램의 내부 구조 파악
- Site
  - http://www.reversecore.com/
  - OllyDbg: http://www.ollydbg.de/





# Hello World! 리버싱



#### Hello World! 프로그램





```
#include "windows.h"
#include "tchar.h"
int _tmain(int argc, TCHAR *argv[])
         MessageBox(NULL,
                               L"Hello World!",
                               L"www.reversecore.com",
                               MB_OK);
         return 0;
```



### HelloWorld.exe 디버깅





 HelloWorld.exe 실행 파일을 디버깅하여 어셈블리 언어로 변환된 main() 함수 찾기