



csbuild for Windows

1조 조별 과제 발표

2016/12/20

공채4기 1조

권도영, 권혁주, 김서현, 박지민, 이용조, 이화중, 임태익

01. 프로젝트 개요

- csbuild 는 소스파일 빌드시 수행되는 컴파일러와 호출시의 인자들을 추출하도록 LD_PRELOAD 후킹 방식을 이용하여 구현된 CODESCROLL 제품내의 Linux 유틸리티이다. LD_PRELOAD 후킹 방식은 Windows 계열에서는 사용할 수 없기 때문에 윈도우용 csbuild 는 다른 방법으로 만들어야 한다.

다행히, 이전 개발자가 시험 삼아 만들었던 코드가 존재한다. 이것을 개량하여 Linux 방식의 csbuild 와 동일한 출력을 내는 프로그램을 개발하라.

➤ 두 줄 요약

- LINUX 버전 csbuild와 동일한 출력을 내는 Windows 버전 csbuild 개발
- 이전 개발자가 시험 삼아 만들었던 코드를 개량하여 개발

➤ 발주일: 2016/12/15 목요일

➤ 마감일: 2016/12/20 화요일

▶ 빌드(Build)

소스 파일은 컴파일러에 의해 컴파일 되어 목적 파일이 되며

목적 파일은 링커에 의해 링크되어 최종적으로 실행 가능한 실행 파일이 되는데 이 전체의 과정을 지칭

▶ 컴파일러 호출시의 인자?

Compile Flag(컴파일 옵션)

ex) gcc -o(출력 결과에 대한 파일명을 지정한다.)

ex) cl -Fm(map 파일을 생성) -GS(버퍼 보안을 체크한다.)

Linker Flag(링커 옵션)

ex) /DEBUG(디버깅 정보를 생성한다.) /DLL(DLL을 빌드한다.)

/PDB(프로그램 데이터베이스 파일을 생성한다.)

▶ LD_PRELOAD 후킹 방식

수행 순서를 Intercept해서 기존의 라이브러리 대신

원하는 라이브러리를 사용하도록 대체할 수 있는 방법

▶ SW 프로젝트 유형이 다름

- 다른 조별 과제는 Greenfield project 또는 Component나 Framework 상에서 개발하는 프로젝트
- 1조의 경우는 기존의 작성된 코드를 수정하는 경우이기 때문에 Evolutionary Project이고 특히 Corrective project

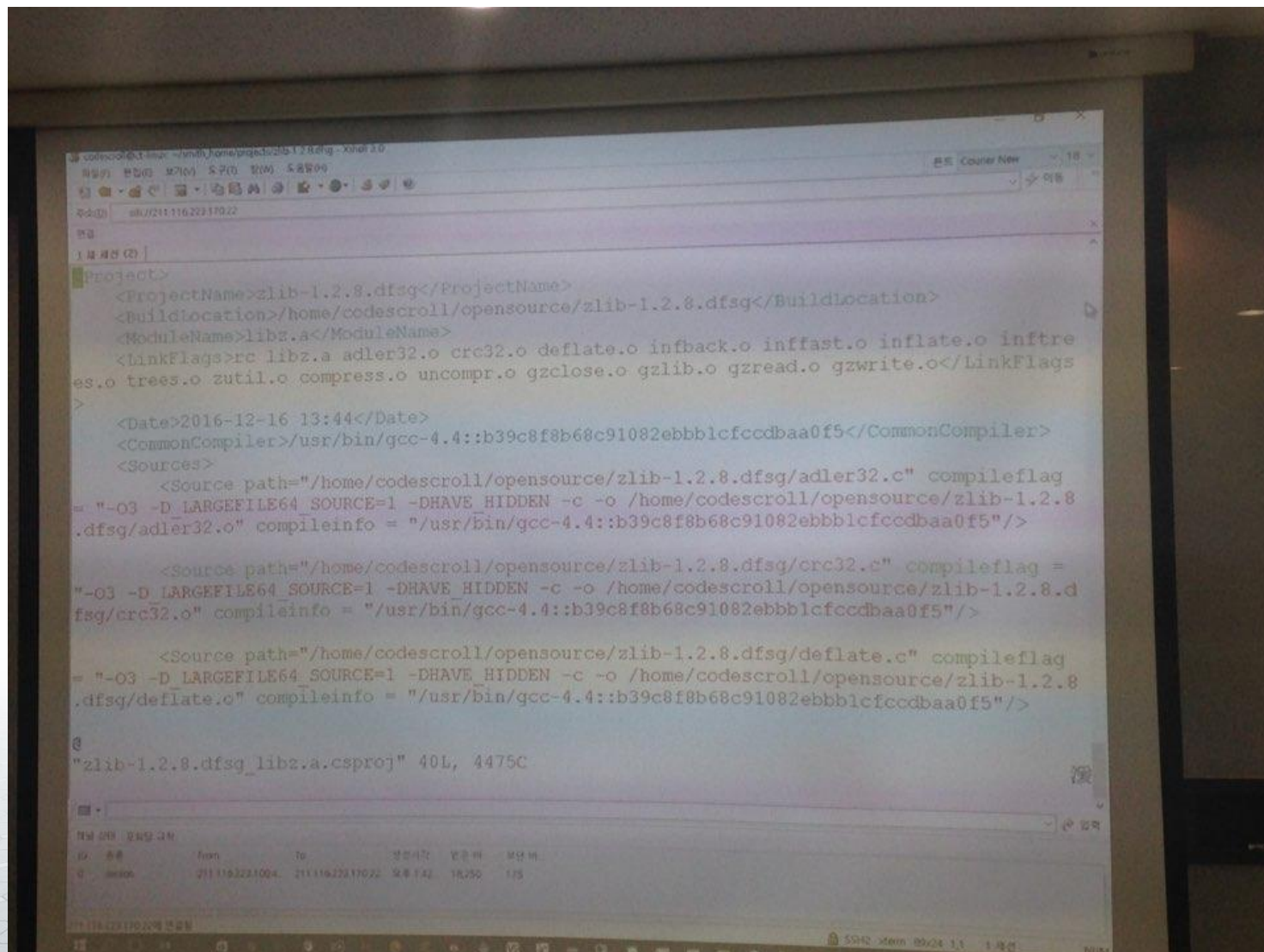
➤ 소프트웨어공학에서 지향하는 개발 프로젝트의 목표와 현재 우리가 수행하는 프로젝트 목표 비교

- 소프트웨어공학에서의 목표

- 1) 납기일 준수(On time)
- 2) 예산 범위 내에서(In budget)
- 3) 품질 높은 소프트웨어를 개발(Quality Software)

- 우리 프로젝트의 목표

- 1) 16년 12월 20일 오후 발표 한 시간 전(오후 4시)까지
- 2) Code Scroll Engine 팀에서 ' 조금 고쳐서 사용해볼까?'라고 생각할만한 *csbuild for Windows* 프로그램 개발



```
<Project>
  <ProjectName>zlib-1.2.8.dfsg</ProjectName>
  <BuildLocation>/home/codescroll/opensource/zlib-1.2.8.dfsg</BuildLocation>
  <ModuleName>libz.a</ModuleName>
  <linkFlags>rc libz.a adler32.o crc32.o deflate.o infback.o inffast.o inflate.o inftre
es.o trees.o zutil.o compress.o uncompr.o gzclose.o gzlib.o gzread.o gzwrite.o</LinkFlags>
  <Date>2016-12-16 13:44</Date>
  <CommonCompiler>/usr/bin/gcc-4.4::b39c8f8b68c91082ebbb1cfccdbaa0f5</CommonCompiler>
  <Sources>
    <Source path="/home/codescroll/opensource/zlib-1.2.8.dfsg/adler32.c" compileflag
    = "-O3 -D_LARGEFILE64_SOURCE=1 -DHAVE_HIDDEN -c -o /home/codescroll/opensource/zlib-1.2.8
    .dfsg/adler32.o" compileinfo = "/usr/bin/gcc-4.4::b39c8f8b68c91082ebbb1cfccdbaa0f5"/>

    <Source path="/home/codescroll/opensource/zlib-1.2.8.dfsg/crc32.c" compileflag =
    "-O3 -D_LARGEFILE64_SOURCE=1 -DHAVE_HIDDEN -c -o /home/codescroll/opensource/zlib-1.2.8.d
    fsg/crc32.o" compileinfo = "/usr/bin/gcc-4.4::b39c8f8b68c91082ebbb1cfccdbaa0f5"/>

    <Source path="/home/codescroll/opensource/zlib-1.2.8.dfsg/deflate.c" compileflag
    = "-O3 -D_LARGEFILE64_SOURCE=1 -DHAVE_HIDDEN -c -o /home/codescroll/opensource/zlib-1.2.8
    .dfsg/deflate.o" compileinfo = "/usr/bin/gcc-4.4::b39c8f8b68c91082ebbb1cfccdbaa0f5"/>
  </Sources>
</Project>
"zlib-1.2.8.dfsg_libz.a.csproj" 40L, 4475C
```


► Usage: : csbuild [compiler] [flags]

<ProjectName></ProjectName>

<BuildLocation></BuildLocation>

<ModuleName></ModuleName>

<LinkFlags></LinkFlags>

<Date></Date>

<CommonCompiler></CommonCompiler>

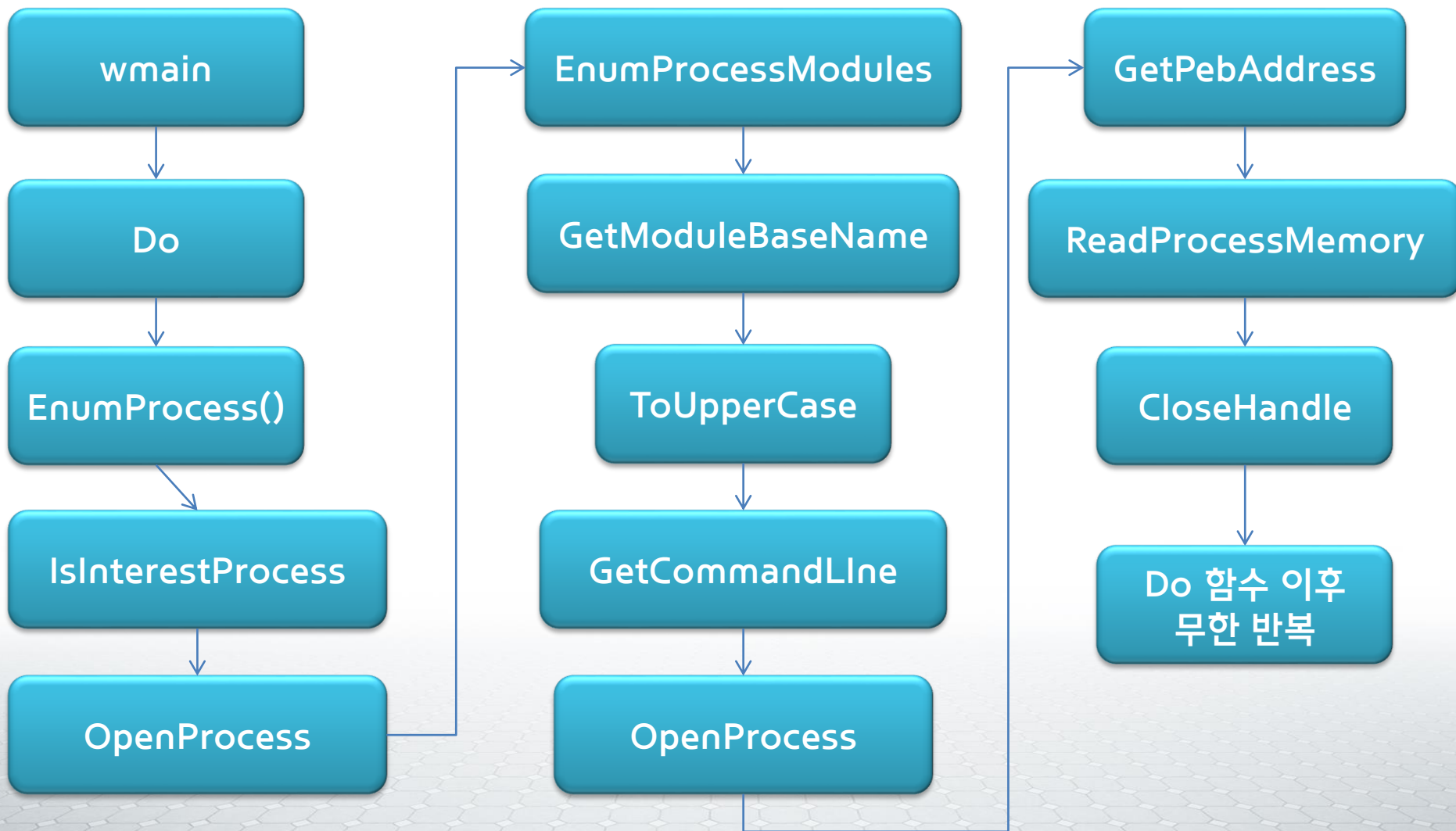
<Sources>

 <Source path="..." />

 <Source path="..." />

 <...>

02. 프로젝트 수행 내용



➤ Issue#1 중복된 결과 출력

-> 한 번 출력되면 더 이상 출력되지 않도록 변경

➤ Issue#2 Compile Flags 찾기

gcc인 경우, 메모리에서 가져온 커맨드 라인이 compile flags라서 찾기 쉬웠는데,
cl(visual studio)의 경우, RSP파일 경로만 나왔다.

-> cl도 gcc와 마찬가지로 메모리에서 정보를 찾아야 되는 줄 알아 혼돈의 도가니

-> 알고 보니 RSP파일에 compile flags가 있었다.

-> RSP파일은 생성되자마자 삭제되는데, 만들어지자마자 내용을 읽어왔다.

➤ Issue#3 절대경로 불러오기

RSP 파일에는 절대경로가 나와있지 않고, 상대경로만 나와있어서 mapping을 할 수 없었다.

-> rtlUserProcParamsAddress + 0x24에 있는

cl, link의 Working Directory의 절대경로를 가져왔다.

➤ Issue#4 Gcc Parser 제작

GccParser 클래스 제작

➤ Issue#5 cl Parser 제작

RspParser 클래스 제작

▶ cl.exe 수행 내역

프로젝트 queue의 빌드를 분석한 결과

```
<Project>
  <ProjectName> queue </ProjectName>
  <BuildLocation> C:\Users\Administrator\Desktop\study\queue\queue\ </BuildLocation>
  <LinkFlags> /OUT:"C:\Users\Administrator\Desktop\study\queue\Debug\queue.exe" /INCREMENTAL /NOLOGO kernel32.lib user32.lib gdi32.lib winspool.lib comdlg32.lib advapi32.lib shell32.lib ole32.lib oleaut32.lib uuid.lib odbccp32.lib /MANIFEST /ManifestFile:"Debug\queue.exe.intermediate.manifest" /MANIFESTUAC:"level='asInvoker' uiAccess='false'" /DEBUG /PDB:"C:\Users\Administrator\Desktop\study\queue\Debug\queue.pdb" /SUBSYSTEM:CONSOLE /TLBID:1 /DYNAMICBASE /NXCOMPAT /IMPLIB:"C:\Users\Administrator\Desktop\study\queue\Debug\queue.lib" /MACHINE:X86 Debug\queue.exe.embed.manifest.res Debug\queue.obj </LinkFlags>
  <CommonCompiler> "C:\Program Files\Microsoft Visual Studio 10.0\VC\bin\CL.exe" </CommonCompiler>
  <Sources>
    <Source name=queue.cpp compileflag=/c /ZI /nologo /W3 /WX- /Od /Oy- /D WIN32 /D _DEBUG /D _CONSOLE /D _UNICODE /D UNICODE /Gm /EHsc /RTC1 /MDd /GS /fp:precise /Zc:wchar_t /Zc:forScope /Fo"Debug\queue.pch" /Fd"Debug\vc100.pdb" /Gd /TP /analyze- /errorReport:prompt />
  </Sources>
</Project>
```

```
/ZI /nologo /W3 /WX- /Od /Oy- /D "WIN32" /D "_DEBUG" /D "_CONSOLE" /D "_UNICODE" /D "UNICODE" /Gm /EHsc /RTC1 /GS /fp:precise /Zc:wchar_t /Zc:forScope /Fp"Debug\queue.pch" /Fa"Debug\queue.pdb" /Fo"Debug\queue.pch" /Fd"Debug\vc100.pdb" /Gd /analyze- /errorReport:queue
```

▶ gpp.exe 수행 내역

test의 빌드를 분석한 결과

```
run: all
    ./test.exe

all: fuck.o test.o
    g++ -o test.exe fuck.o test.o

fuck.o: fuck.cpp
    g++ -c fuck.cpp

test.o: test.cpp
    g++ -c test.cpp

clean:
    del *.o test.exe
```

```
C:\#Users#Tae-Ik\Desktop>make all
g++ -c fuck.cpp
g++ -c test.cpp
g++ -o test.exe fuck.o test.o

C:\#Users#Tae-Ik\Desktop>
```

```
<Project>
  <ProjectName>test</ProjectName>
  <BuildLocation>C:\#Users#Tae-Ik\Desktop#\</BuildLocation>
  <LinkFlags>g++ -o test.exe fuck.o test.o</LinkFlags>
  <Sources>
    <Source name="fuck.cpp" compileFlag="-c" />
    <Source name="test.cpp" compileFlag="-c" />
  </Sources>
</Project>
```

▶ 이름(기여도(%))

권민혁 팀장님(1)

임태익(25)

권도영(20)

권혁주(14)

김서현(10)

박지민(10)

이용조(10)

이화중(10)

03. 시연

Thank you for your kind attention



NOTICE: Proprietary and Confidential

This material is proprietary to Suresoft Technologies, Inc..

It contains trade secret and confidential information which is solely the property of Suresoft Technologies, Inc.

This material is for client's internal use only. This material shall not be used, reproduced, copied,

disclosed, transmitted, in whole or in part, without the express consent of Suresoft Technologies, Inc.

Copyright © 2016 by Suresoft Technologies, Inc., All rights reserved.

www.suresofttech.com www.codescroll.com • •