GCC & GDB

Linux

목차

- gcc란
- gcc의 옵션 & 간단한 예제
- gdb
- gdb 문제

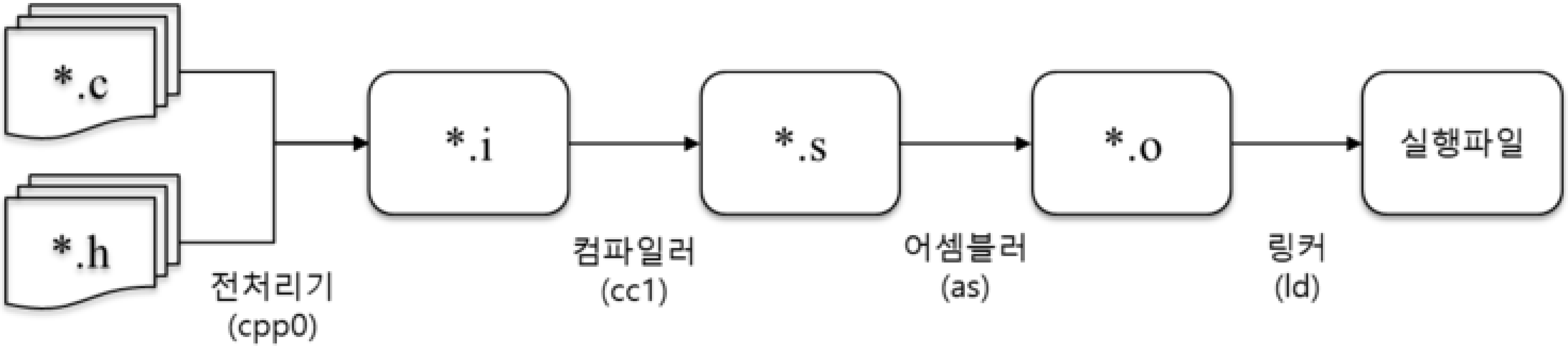
gcc란

GNU 컴파일러 모음

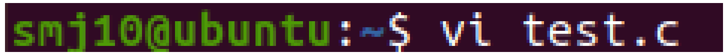
리눅스 컴파일러

여러 언어를 컴파일

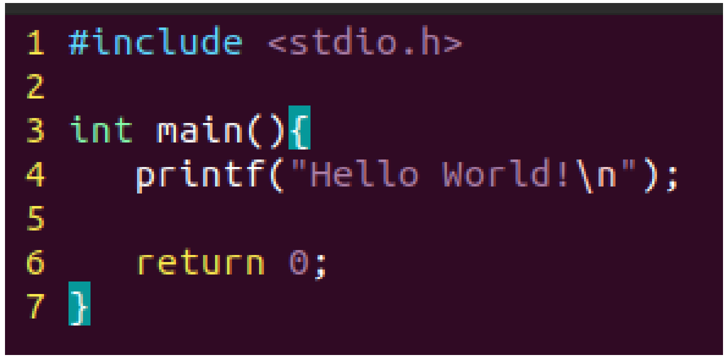
gcc란 - 컴파일 과정



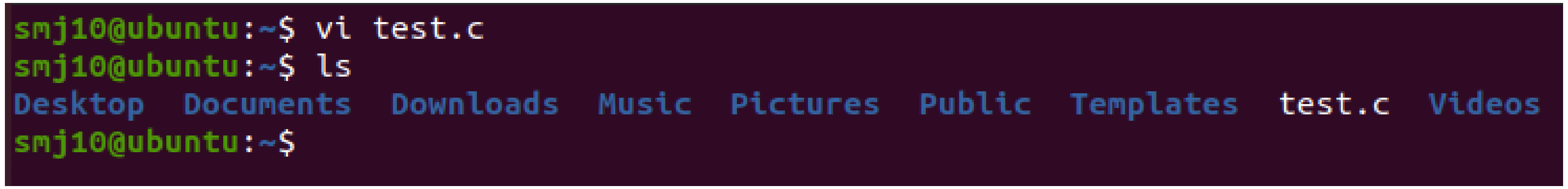
gcc의 옵션 & 간단한 예제



```
smj10@ubuntu:~$ vi test.c
```

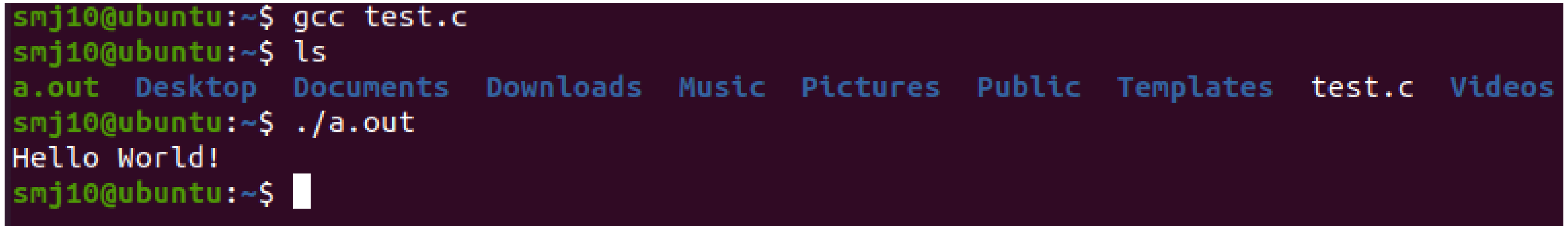


```c
#include <stdio.h>

int main(){
    printf("Hello World!\n");

    return 0;
}
```



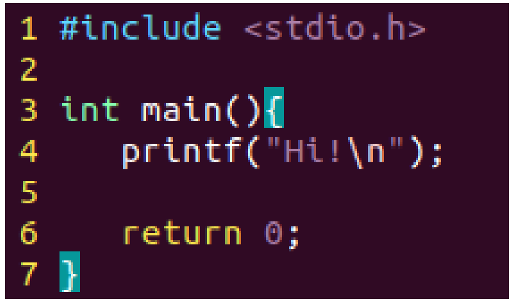
```
smj10@ubuntu:~$ vi test.c
smj10@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  test.c  Videos
smj10@ubuntu:~$
```

gcc의 옵션 & 간단한 예제

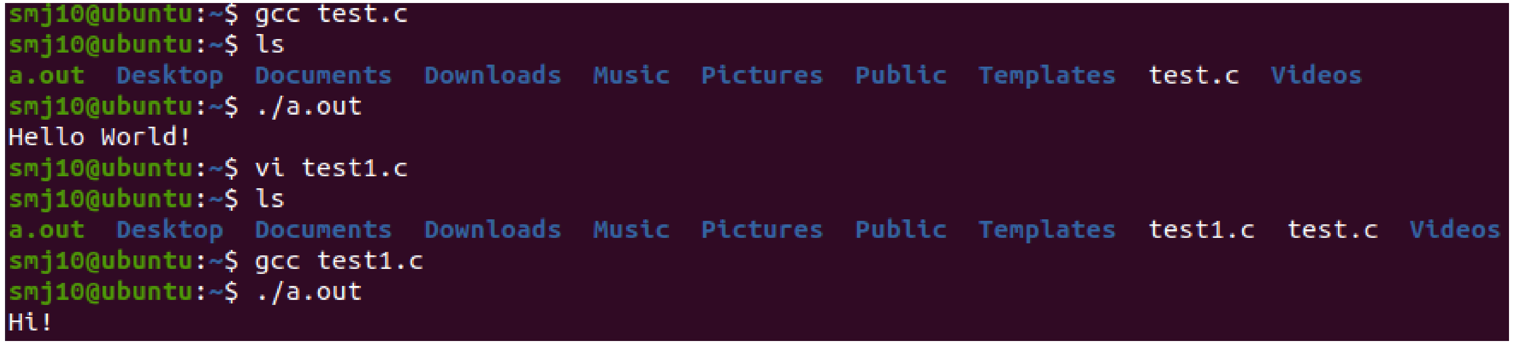


```
smj10@ubuntu:~$ gcc test.c
smj10@ubuntu:~$ ls
a.out  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  test.c  Videos
smj10@ubuntu:~$ ./a.out
Hello World!
smj10@ubuntu:~$ 
```

gcc의 옵션 & 간단한 예제

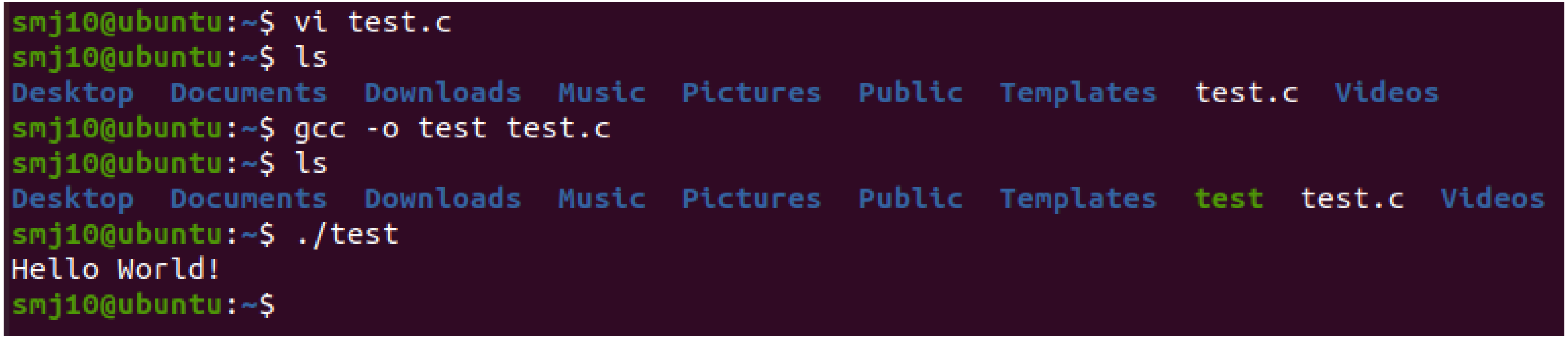


```c
#include <stdio.h>

int main(){
    printf("Hi!\n");

    return 0;
}
```



```
smj10@ubuntu:~$ gcc test.c
smj10@ubuntu:~$ ls
a.out  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  test.c  Videos
smj10@ubuntu:~$ ./a.out
Hello World!
smj10@ubuntu:~$ vi test1.c
smj10@ubuntu:~$ ls
a.out  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  test1.c  test.c  Videos
smj10@ubuntu:~$ gcc test1.c
smj10@ubuntu:~$ ./a.out
Hi!
```

gcc의 옵션 & 간단한 예제



```
smj10@ubuntu:~$ vi test.c
smj10@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  test.c  Videos
smj10@ubuntu:~$ gcc -o test test.c
smj10@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  test  test.c  Videos
smj10@ubuntu:~$ ./test
Hello World!
smj10@ubuntu:~$
```

gcc의 옵션 & 간단한 예제

--save-temps : 컴파일시 생성되는 중간 파일 저장

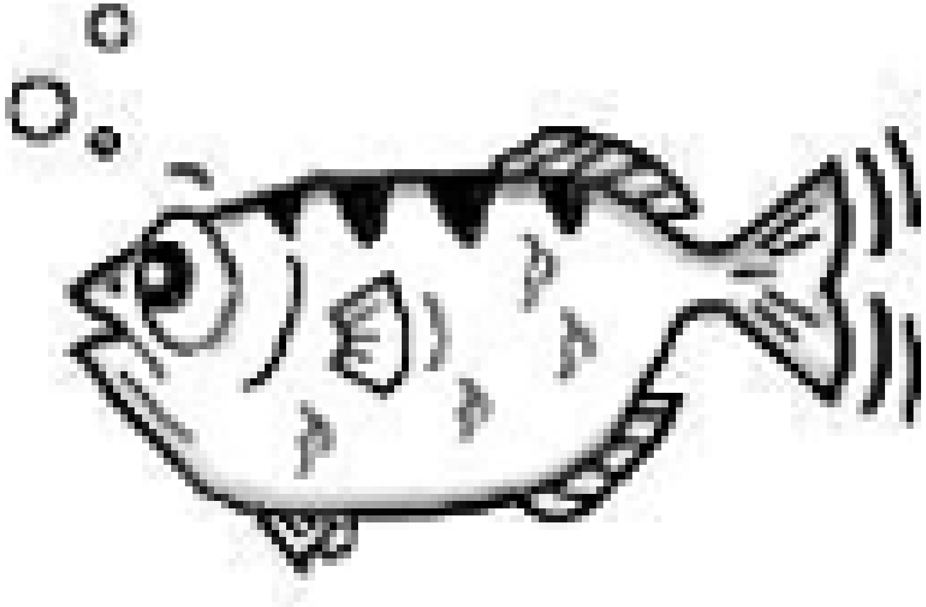
-v : 컴파일 과정을 화면에 출력

-E 옵션 : 전처리 과정의 결과를 화면에 보이는 옵션

-S : 어셈블리 파일 생성

-c : 오브젝트 파일 생성

gdb

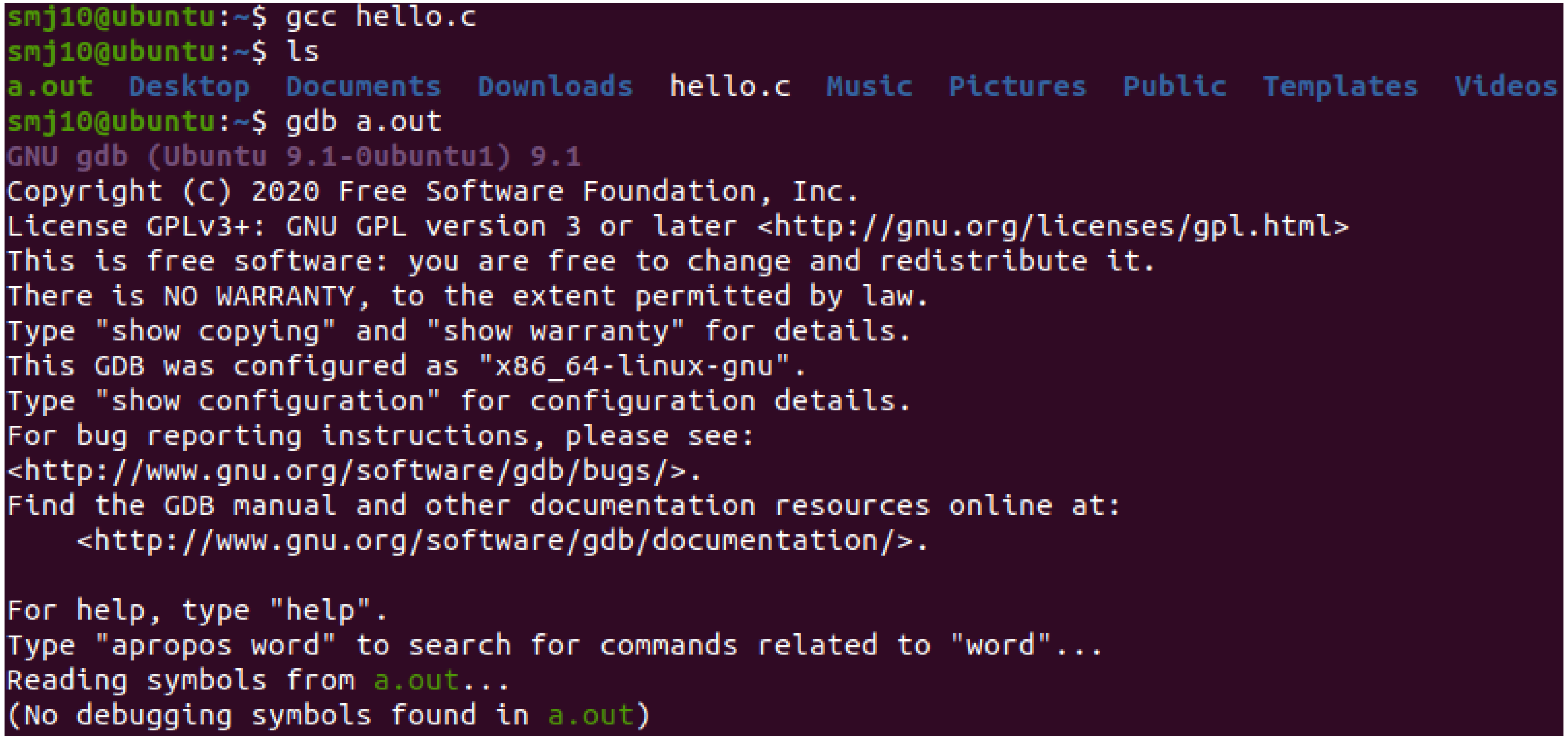


GNU 디버거

유닉스 기반의 시스템에서 동작

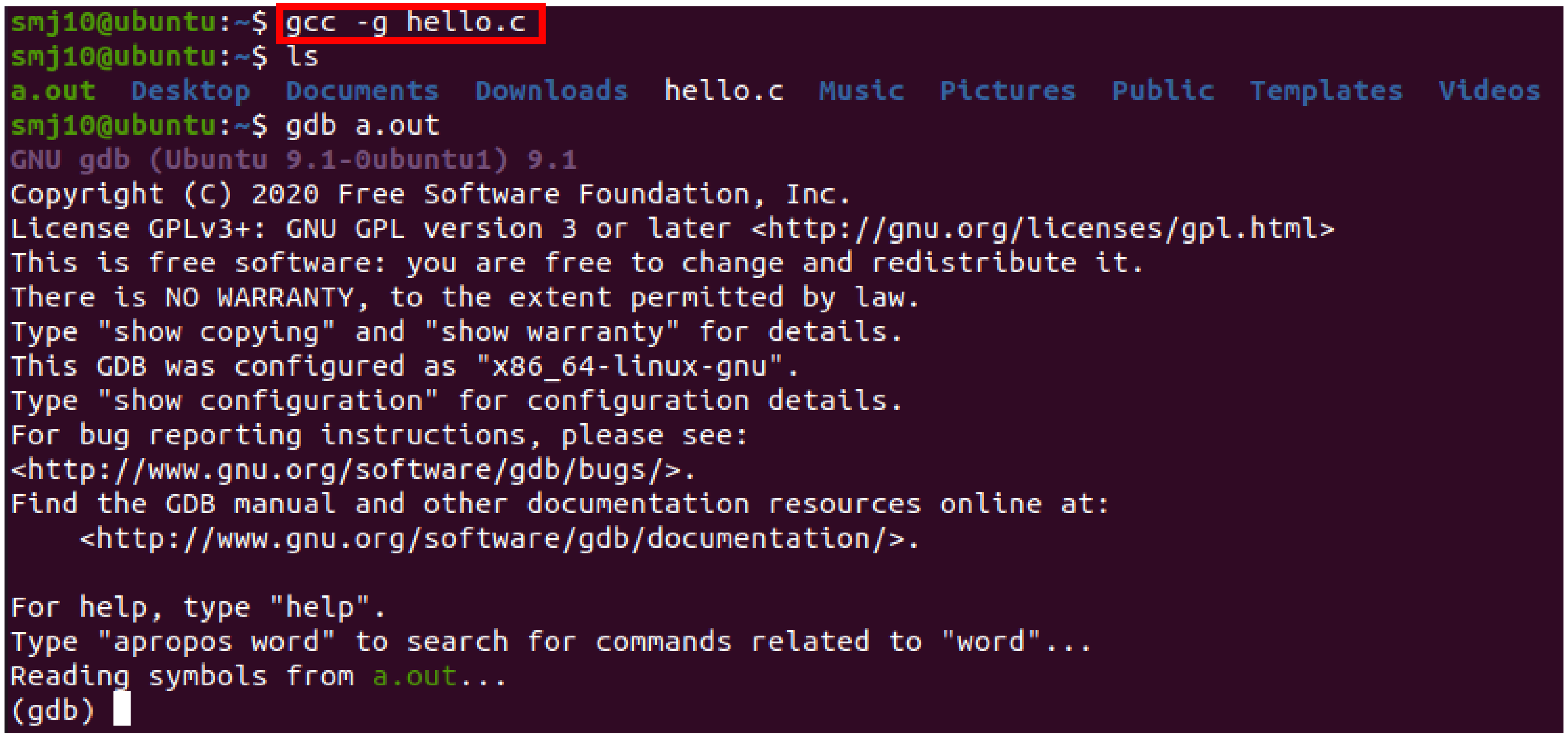
여러 프로그래밍 언어를 지원

gdb



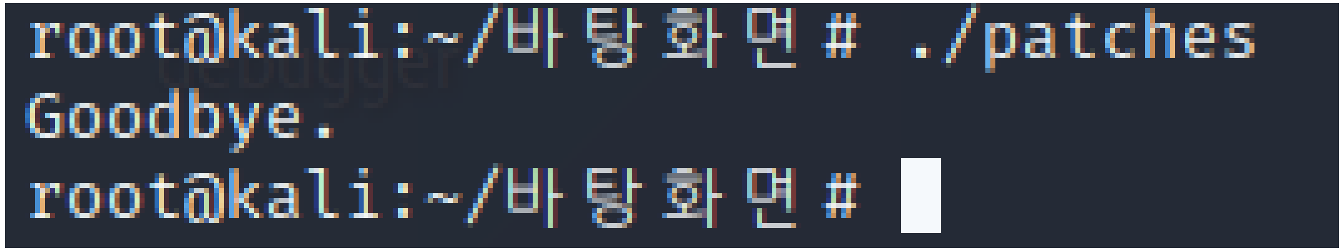
```
smj10@ubuntu:~$ gcc hello.c
smj10@ubuntu:~$ ls
a.out  Desktop  Documents  Downloads  hello.c  Music  Pictures  Public  Templates  Videos
smj10@ubuntu:~$ gdb a.out
GNU gdb (Ubuntu 9.1-0ubuntu1) 9.1
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from a.out...
(No debugging symbols found in a.out)
```

gdb



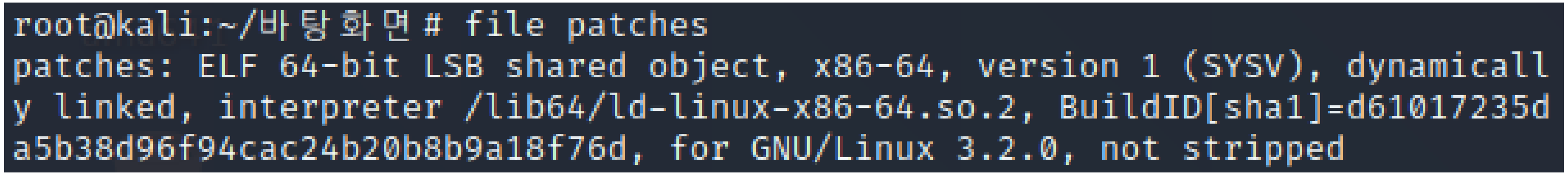
```
smj10@ubuntu:~$ gcc -g hello.c
smj10@ubuntu:~$ ls
a.out  Desktop  Documents  Downloads  hello.c  Music  Pictures  Public  Templates  Videos
smj10@ubuntu:~$ gdb a.out
GNU gdb (Ubuntu 9.1-0ubuntu1) 9.1
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from a.out...
(gdb) 
```

gdb 문제



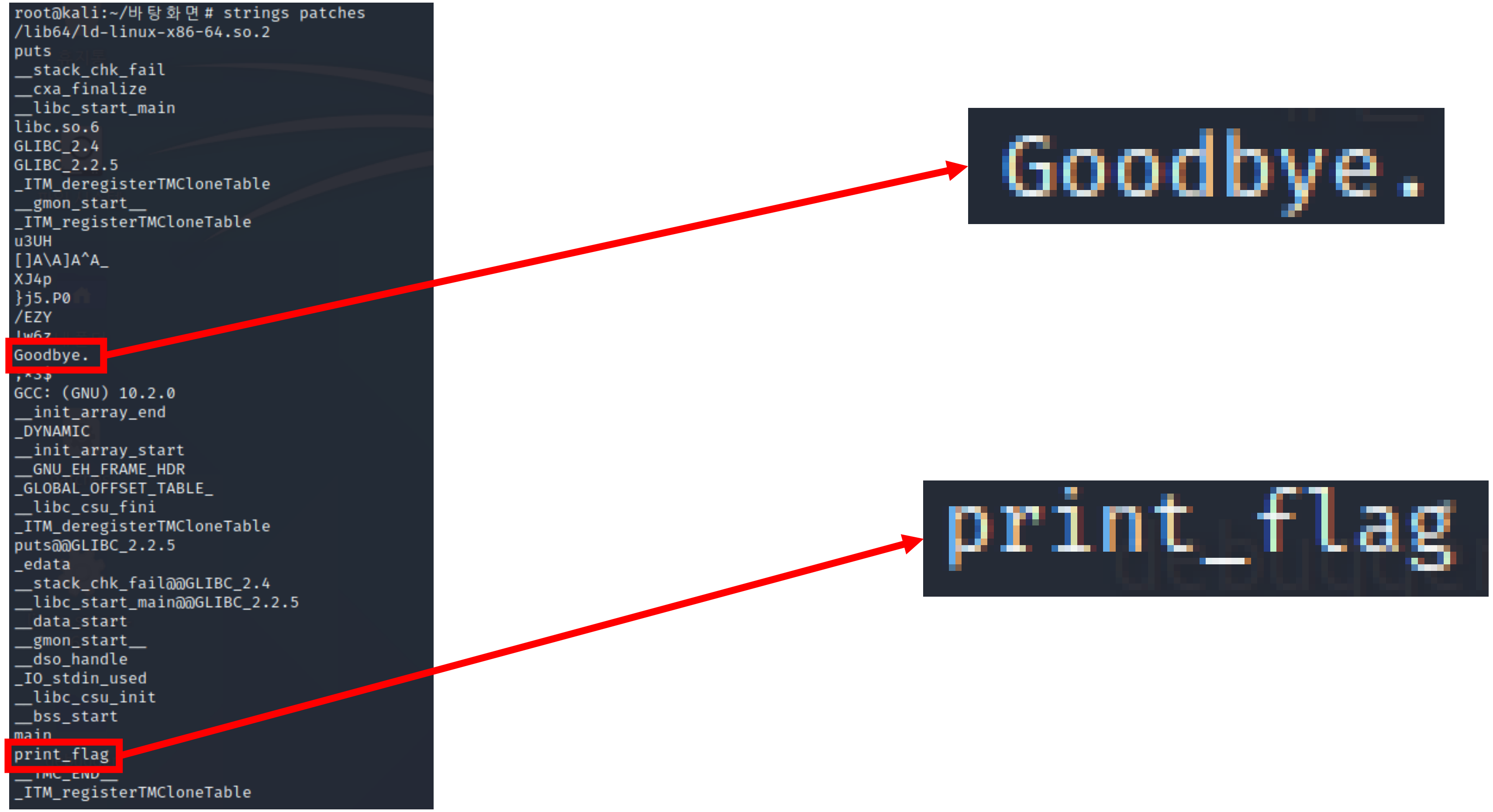
```
root@kali:~/바탕화면# ./patches
Goodbye.
root@kali:~/바탕화면# 
```

gdb 문제



```
root@kali:~/바탕화면# file patches
patches: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamicall
y linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=d61017235d
a5b38d96f94cac24b20b8b9a18f76d, for GNU/Linux 3.2.0, not stripped
```

gdb 문제

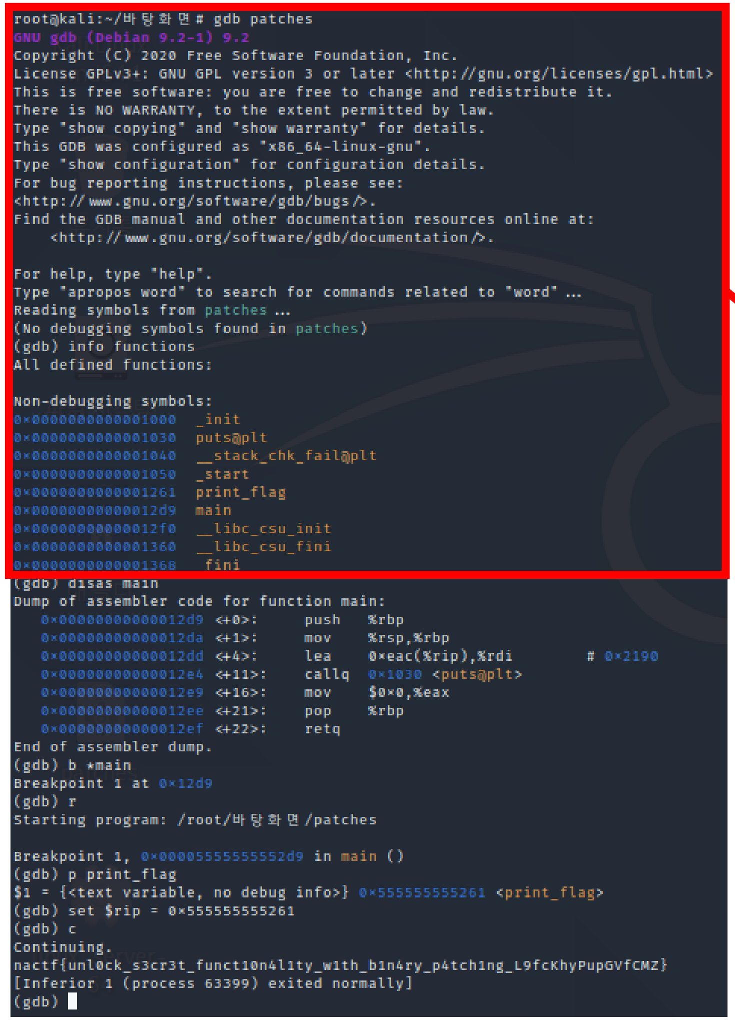


```
root@kali:~/바탕화면# strings patches
/lib64/ld-linux-x86-64.so.2
puts
__stack_chk_fail
__cxa_finalize
__libc_start_main
libc.so.6
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u3UH
[]A\A]A^A_
XJ4p
}j5.P0
/EZY
!w6z
Goodbye.
;*3$
GCC: (GNU) 10.2.0
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
puts@@GLIBC_2.2.5
_edata
__stack_chk_fail@@GLIBC_2.4
__libc_start_main@@GLIBC_2.2.5
__data_start
__gmon_start__
__dso_handle
_IO_stdin_used
__libc_csu_init
__bss_start
main
print_flag
__TMC_END__
_ITM_registerTMCloneTable
```

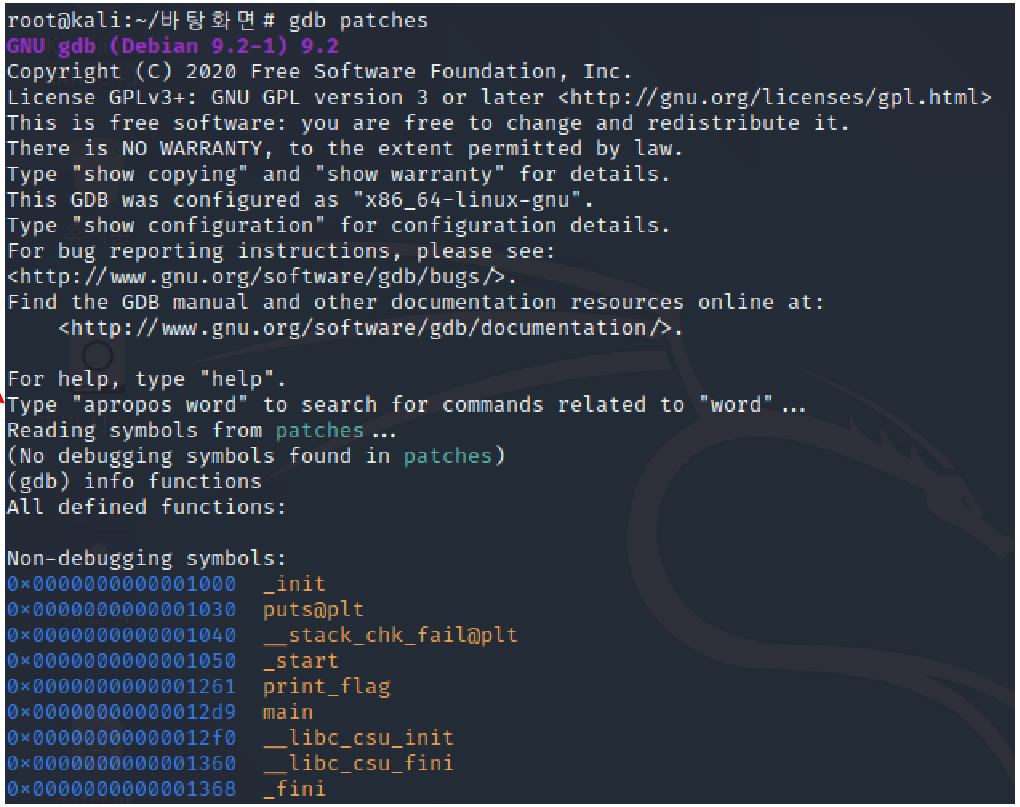
```
Goodbye.
```

```
print_flag
```

gdb 문제

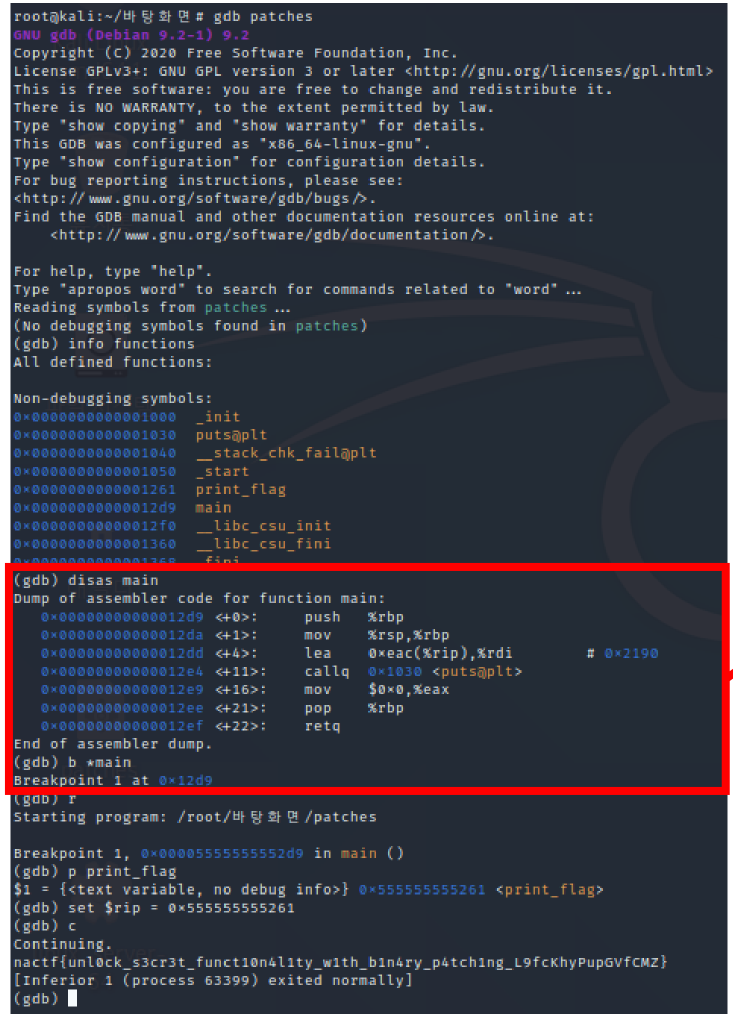


```
root@kali:~/바탕화면# gdb patches
GNU gdb (Debian 9.2-1) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from patches...
(No debugging symbols found in patches)
(gdb) info functions
All defined functions:

Non-debugging symbols:
0x0000000000001000  _init
0x0000000000001030  puts@plt
0x0000000000001040  __stack_chk_fail@plt
0x0000000000001050  _start
0x0000000000001261  print_flag
0x00000000000012d9  main
0x00000000000012f0  __libc_csu_init
0x0000000000001360  __libc_csu_fini
0x0000000000001368  _fini
(gdb) disas main
Dump of assembler code for function main:
   0x00000000000012d9 <+0>:     push   %rbp
   0x00000000000012da <+1>:     mov    %rsp,%rbp
   0x00000000000012dd <+4>:     lea    0xeac(%rip),%rdi        # 0x2190
   0x00000000000012e4 <+11>:    callq  0x1030 <puts@plt>
   0x00000000000012e9 <+16>:    mov    $0x0,%eax
   0x00000000000012ee <+21>:    pop    %rbp
   0x00000000000012ef <+22>:    retq
End of assembler dump.
(gdb) b *main
Breakpoint 1 at 0x12d9
(gdb) r
Starting program: /root/바탕화면/patches

Breakpoint 1, 0x00005555555552d9 in main ()
(gdb) p print_flag
$1 = {<text variable, no debug info>} 0x555555555261 <print_flag>
(gdb) set $rip = 0x555555555261
(gdb) c
Continuing.
nactf{unl0ck_s3cr3t_funct10n4l1ty_w1th_b1n4ry_p4tch1ng_L9fcKhyPupGVfCMZ}
[Inferior 1 (process 63399) exited normally]
(gdb) 
```

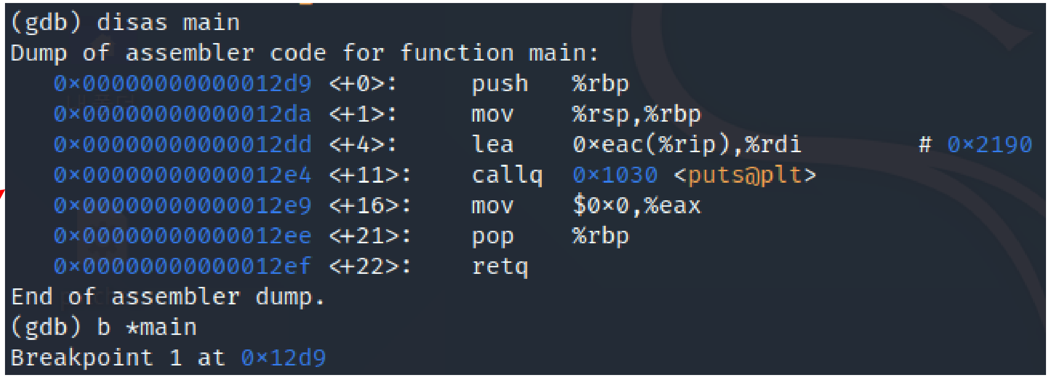


```
root@kali:~/바탕화면# gdb patches
GNU gdb (Debian 9.2-1) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from patches...
(No debugging symbols found in patches)
(gdb) info functions
All defined functions:

Non-debugging symbols:
0x0000000000001000  _init
0x0000000000001030  puts@plt
0x0000000000001040  __stack_chk_fail@plt
0x0000000000001050  _start
0x0000000000001261  print_flag
0x00000000000012d9  main
0x00000000000012f0  __libc_csu_init
0x0000000000001360  __libc_csu_fini
0x0000000000001368  _fini
```

gdb 문제

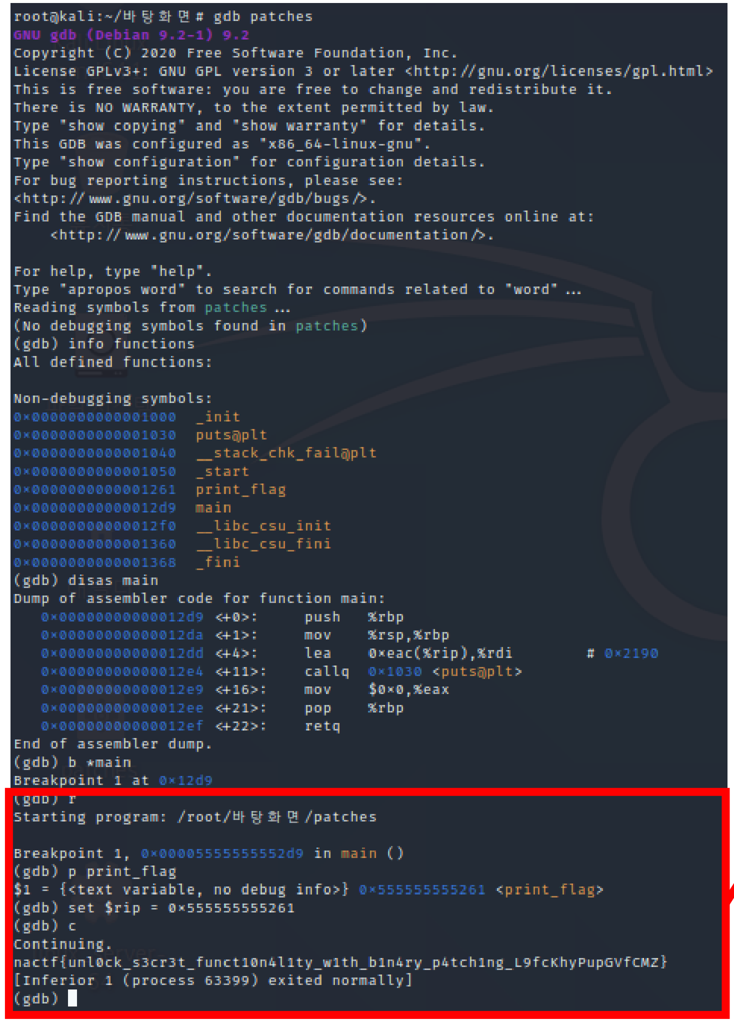


```
root@kali:~/바탕화면# gdb patches
GNU gdb (Debian 9.2-1) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word" ...
Reading symbols from patches ...
(No debugging symbols found in patches)
(gdb) info functions
All defined functions:

Non-debugging symbols:
0x0000000000001000  _init
0x0000000000001030  puts@plt
0x0000000000001040  __stack_chk_fail@plt
0x0000000000001050  _start
0x0000000000001261  print_flag
0x00000000000012d9  main
0x00000000000012f0  __libc_csu_init
0x0000000000001360  __libc_csu_fini
0x0000000000001368  _fini
(gdb) disas main
Dump of assembler code for function main:
   0x00000000000012d9 <+0>:     push   %rbp
   0x00000000000012da <+1>:     mov    %rsp,%rbp
   0x00000000000012dd <+4>:     lea    0xeac(%rip),%rdi        # 0x2190
   0x00000000000012e4 <+11>:    callq  0x1030 <puts@plt>
   0x00000000000012e9 <+16>:    mov    $0x0,%eax
   0x00000000000012ee <+21>:    pop    %rbp
   0x00000000000012ef <+22>:    retq
End of assembler dump.
(gdb) b *main
Breakpoint 1 at 0x12d9
(gdb) r
Starting program: /root/바탕화면/patches

Breakpoint 1, 0x00005555555552d9 in main ()
(gdb) p print_flag
$1 = {<text variable, no debug info>} 0x555555555261 <print_flag>
(gdb) set $rip = 0x555555555261
(gdb) c
Continuing.
nactf{unl0ck_s3cr3t_funct10n4l1ty_w1th_b1n4ry_p4tch1ng_L9fcKhyPupGVfCMZ}
[Inferior 1 (process 63399) exited normally]
(gdb) 
```

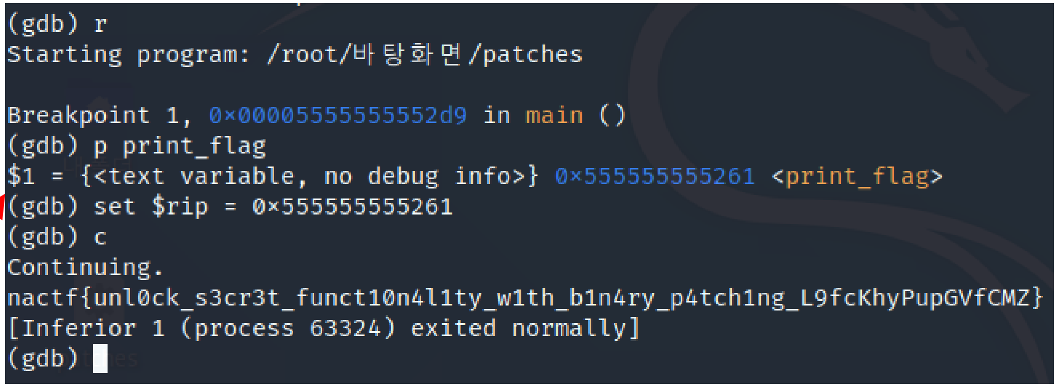


```
(gdb) disas main
Dump of assembler code for function main:
   0x00000000000012d9 <+0>:     push   %rbp
   0x00000000000012da <+1>:     mov    %rsp,%rbp
   0x00000000000012dd <+4>:     lea    0xeac(%rip),%rdi        # 0x2190
   0x00000000000012e4 <+11>:    callq  0x1030 <puts@plt>
   0x00000000000012e9 <+16>:    mov    $0x0,%eax
   0x00000000000012ee <+21>:    pop    %rbp
   0x00000000000012ef <+22>:    retq
End of assembler dump.
(gdb) b *main
Breakpoint 1 at 0x12d9
```

gdb 문제



```
root@kali:~/바탕화면# gdb patches
GNU gdb (Debian 9.2-1) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from patches...
(No debugging symbols found in patches)
(gdb) info functions
All defined functions:

Non-debugging symbols:
0x0000000000001000  _init
0x0000000000001030  puts@plt
0x0000000000001040  __stack_chk_fail@plt
0x0000000000001050  _start
0x0000000000001261  print_flag
0x00000000000012d9  main
0x00000000000012f0  __libc_csu_init
0x0000000000001360  __libc_csu_fini
0x0000000000001368  _fini
(gdb) disas main
Dump of assembler code for function main:
   0x00000000000012d9 <+0>:     push   %rbp
   0x00000000000012da <+1>:     mov    %rsp,%rbp
   0x00000000000012dd <+4>:     lea    0xeac(%rip),%rdi        # 0x2190
   0x00000000000012e4 <+11>:    callq  0x1030 <puts@plt>
   0x00000000000012e9 <+16>:    mov    $0x0,%eax
   0x00000000000012ee <+21>:    pop    %rbp
   0x00000000000012ef <+22>:    retq
End of assembler dump.
(gdb) b *main
Breakpoint 1 at 0x12d9
(gdb) r
Starting program: /root/바탕화면/patches

Breakpoint 1, 0x00005555555552d9 in main ()
(gdb) p print_flag
$1 = {<text variable, no debug info>} 0x555555555261 <print_flag>
(gdb) set $rip = 0x555555555261
(gdb) c
Continuing.
nactf{unl0ck_s3cr3t_funct10n4l1ty_w1th_b1n4ry_p4tch1ng_L9fcKhyPupGVfCMZ}
[Inferior 1 (process 63399) exited normally]
(gdb) 
```



```
(gdb) r
Starting program: /root/바탕화면/patches

Breakpoint 1, 0x00005555555552d9 in main ()
(gdb) p print_flag
$1 = {<text variable, no debug info>} 0x555555555261 <print_flag>
(gdb) set $rip = 0x555555555261
(gdb) c
Continuing.
nactf{unl0ck_s3cr3t_funct10n4l1ty_w1th_b1n4ry_p4tch1ng_L9fcKhyPupGVfCMZ}
[Inferior 1 (process 63324) exited normally]
(gdb) 
```

gdb 문제 - 스택 프레임

1.함수가 사용할 파라미터를 스택에 넣고 함수 시작지점으로 점프(함수 호출)한다.
2.함수 내에서 사용할 스택프레임을 설정한다. (프롤로그)
3.함수의 내용을 수행한다.
4.수행을 마치고 처음 호출한 지점으로 돌아가기 위해 스택을 복원한다(에필로그)

gdb 문제 스택 프레임

프롤로그

```
PUSH EBP          ; 함수시작(EBP를 사용하기 전에 초기 값을 스택에 저장)
MOV EBP, ESP      ; 현재의 ESP를 EBP에 저장
```

```
                  ; 함수의 본체
...               ; 여기서 ESP가 변경되더라도 EBP가 변경되지 않으므로
                  ; 안전하게 로컬변수와 파라미터를 엑세스할 수 있음
```

에필로그

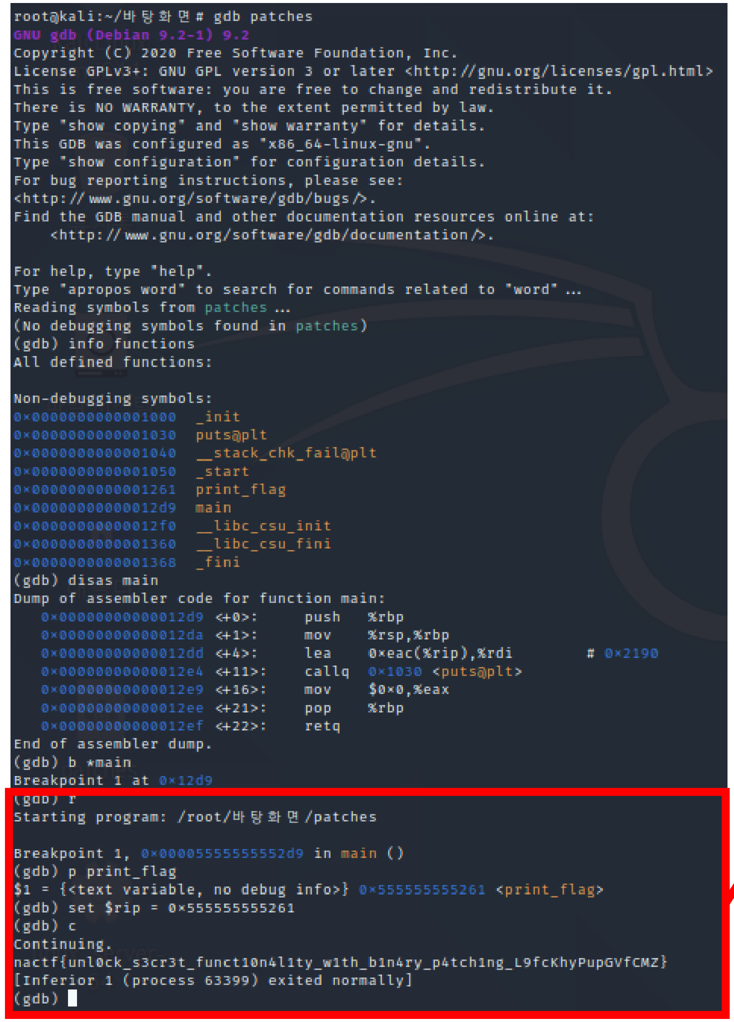
```
MOV ESP, EBP      ; ESP를 정리(함수가 시작했을 때의 초기값으로 복원)
POP EBP           ; 리턴되기 전에 저장해 놓았던 원래 EBP 값으로 복원
RETN              ; 함수 종료
```

gdb 문제 - 스택 프레임

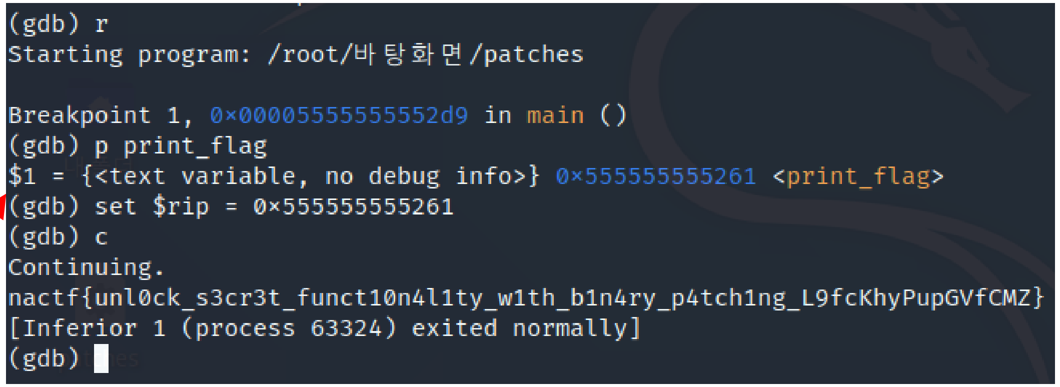
```
MOV ESP, EBP      ; ESP를 정리(함수가 시작했을 때의 초기값으로 복원)
POP EBP           ; 리턴되기 전에 저장해 놓았던 원래 EBP 값으로 복원
RETN              ; 함수 종료
```

pop EIP
jmp EIP

gdb 문제



```
root@kali:~/바탕화면# gdb patches
GNU gdb (Debian 9.2-1) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from patches...
(No debugging symbols found in patches)
(gdb) info functions
All defined functions:

Non-debugging symbols:
0x0000000000001000  _init
0x0000000000001030  puts@plt
0x0000000000001040  __stack_chk_fail@plt
0x0000000000001050  _start
0x0000000000001261  print_flag
0x00000000000012d9  main
0x00000000000012f0  __libc_csu_init
0x0000000000001360  __libc_csu_fini
0x0000000000001368  _fini
(gdb) disas main
Dump of assembler code for function main:
   0x00000000000012d9 <+0>:     push   %rbp
   0x00000000000012da <+1>:     mov    %rsp,%rbp
   0x00000000000012dd <+4>:     lea    0xeac(%rip),%rdi        # 0x2190
   0x00000000000012e4 <+11>:    callq  0x1030 <puts@plt>
   0x00000000000012e9 <+16>:    mov    $0x0,%eax
   0x00000000000012ee <+21>:    pop    %rbp
   0x00000000000012ef <+22>:    retq
End of assembler dump.
(gdb) b *main
Breakpoint 1 at 0x12d9
(gdb) r
Starting program: /root/바탕화면/patches

Breakpoint 1, 0x00005555555552d9 in main ()
(gdb) p print_flag
$1 = {<text variable, no debug info>} 0x555555555261 <print_flag>
(gdb) set $rip = 0x555555555261
(gdb) c
Continuing.
nactf{unl0ck_s3cr3t_funct10n4l1ty_w1th_b1n4ry_p4tch1ng_L9fcKhyPupGVfCMZ}
[Inferior 1 (process 63399) exited normally]
(gdb) 
```



```
(gdb) r
Starting program: /root/바탕화면/patches

Breakpoint 1, 0x00005555555552d9 in main ()
(gdb) p print_flag
$1 = {<text variable, no debug info>} 0x555555555261 <print_flag>
(gdb) set $rip = 0x555555555261
(gdb) c
Continuing.
nactf{unl0ck_s3cr3t_funct10n4l1ty_w1th_b1n4ry_p4tch1ng_L9fcKhyPupGVfCMZ}
[Inferior 1 (process 63324) exited normally]
(gdb) 
```

감사합니다