Lab 3: Binary Bomb Lab

KAIST CS230 Fall 2020

Due: Mon 12th, Oct 2020
23:59:59 KST

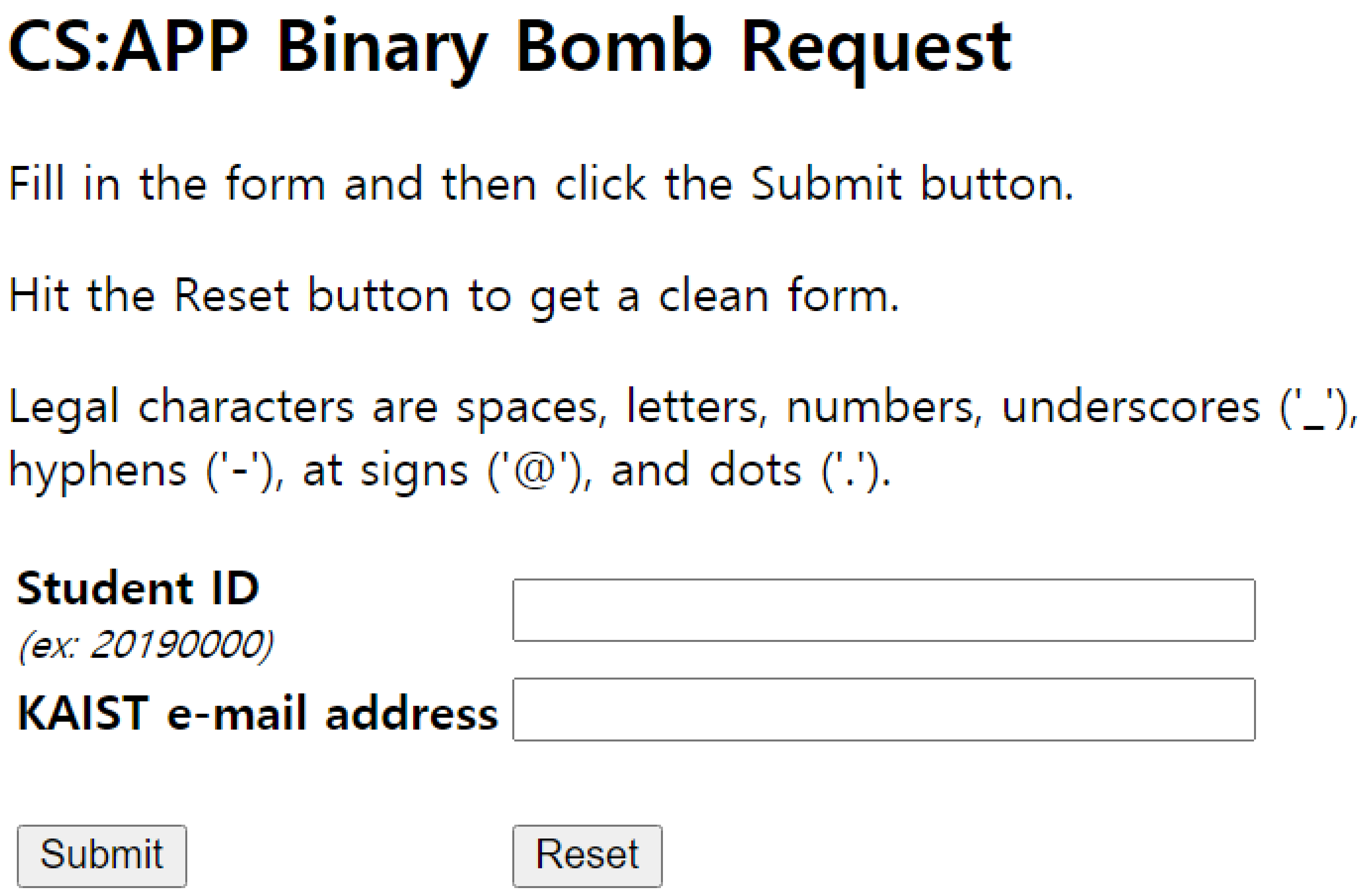
Overview

- The ‘bomb’ file is a binary executable file.
- Bomb includes 6 stages to defuse + 1 hidden stage
- Only main routine will be given as source code.

Preparing Workspace

- Get bomb at http://143.248.188.188:15213
  - It will be downloaded as .tar file
- Move .tar file to your linux server
  - You will need to use scp tools
- Decompress .tar file by typing ‘tar –xvf <file name>’
- Now, deal with bomb under generated directory!

Bomb Request Webpage



CS:APP Binary Bomb Request

Fill in the form and then click the Submit button.

Hit the Reset button to get a clean form.

Legal characters are spaces, letters, numbers, underscores ('_'), hyphens ('-'), at signs ('@'), and dots ('.').

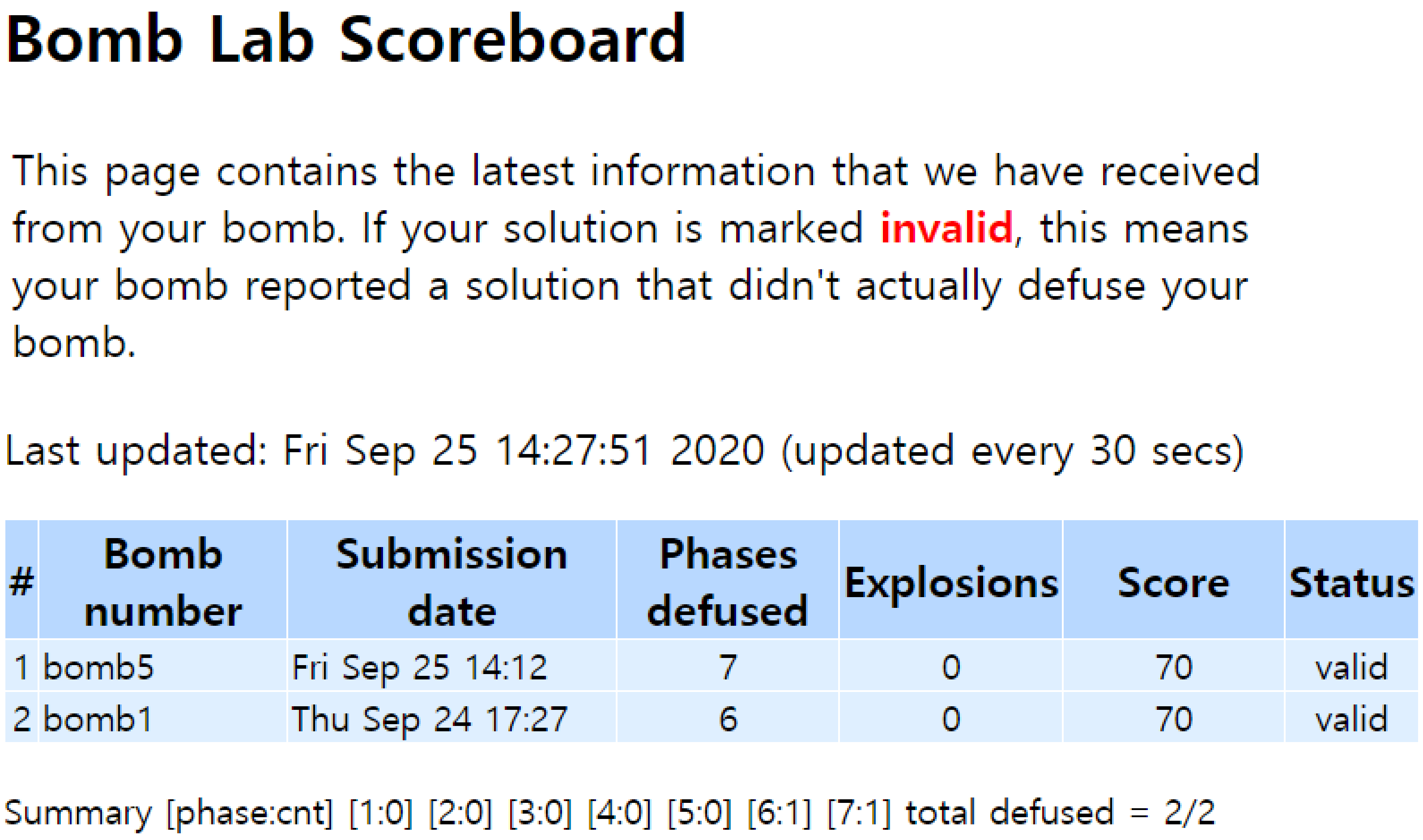
Student ID
(ex: 20190000)

KAIST e-mail address

Submission

- Unlike previous labs, we’re not using gitlab.
- Check your score at http://143.248.188.188:15213/scoreboard
- This time, you don’t need to submit your solution.
- Just defuse your bomb at provided linux server!

Scoreboard Webpage



Bomb Lab Scoreboard

This page contains the latest information that we have received from your bomb. If your solution is marked **invalid**, this means your bomb reported a solution that didn't actually defuse your bomb.

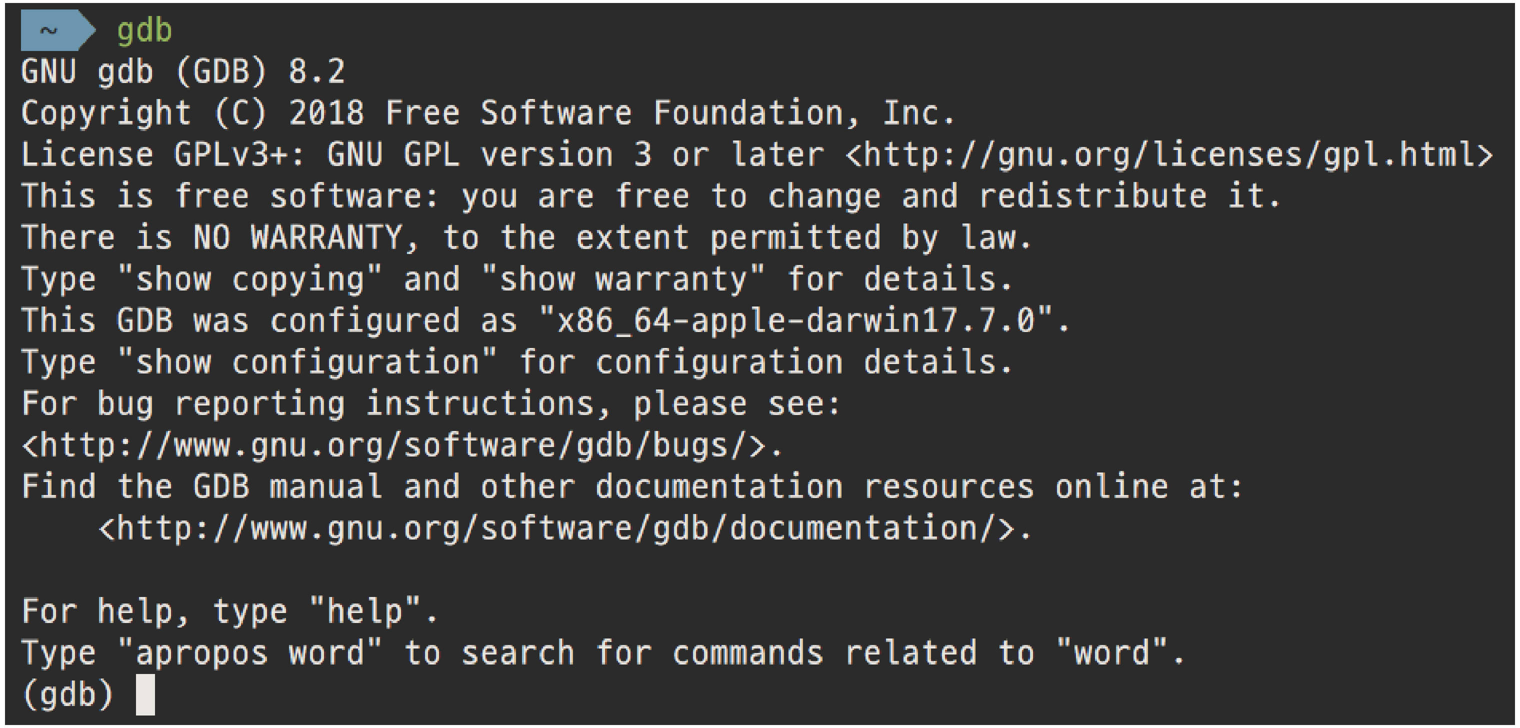
Last updated: Fri Sep 25 14:27:51 2020 (updated every 30 secs)

#	Bomb number	Submission date	Phases defused	Explosions	Score	Status
1	bomb5	Fri Sep 25 14:12	7	0	70	valid
2	bomb1	Thu Sep 24 17:27	6	0	70	valid

Summary [phase:cnt] [1:0] [2:0] [3:0] [4:0] [5:0] [6:1] [7:1] total defused = 2/2

Tools - GDB

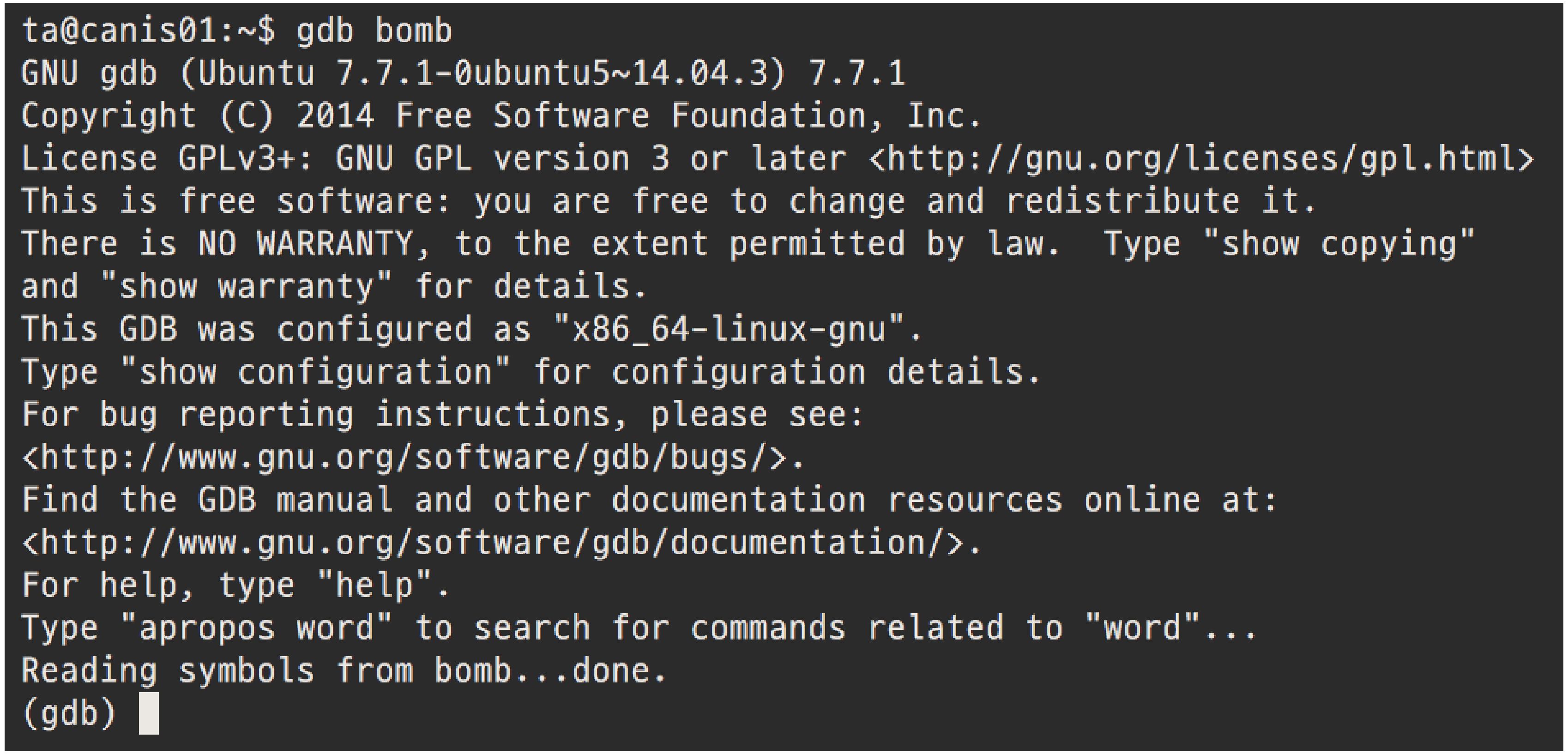
- GNU Debugger
- Shows machine state in real time



```
 ~  gdb
GNU gdb (GDB) 8.2
Copyright (C) 2018 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-apple-darwin17.7.0".
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".
(gdb) 
```

Tools - GDB

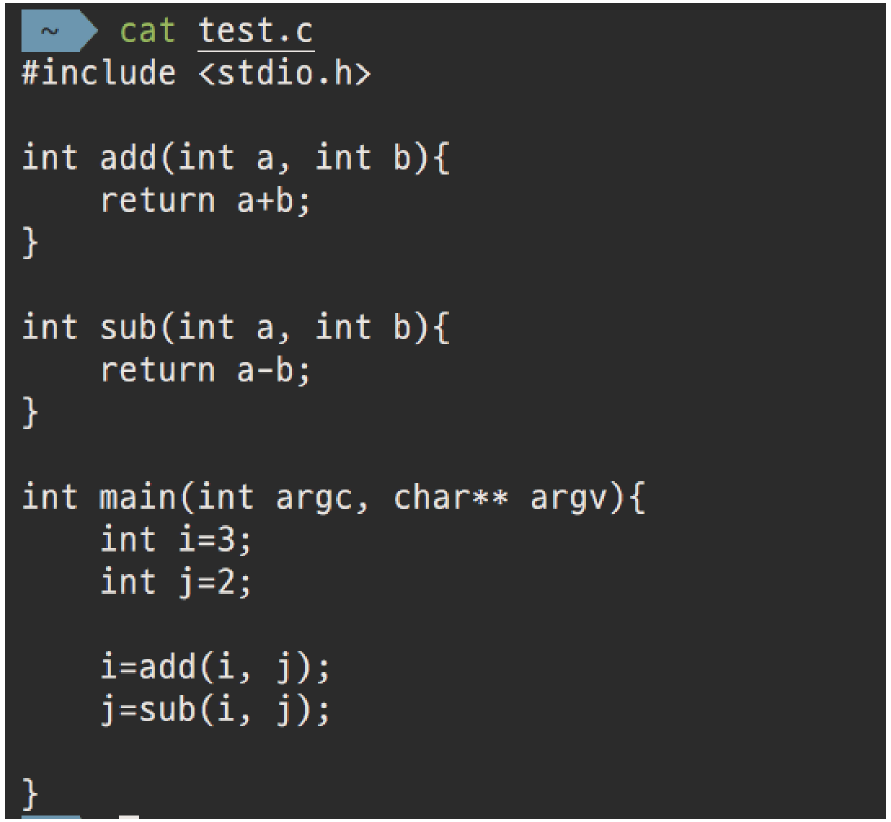
- Start GDB: gdb [options] [executable name]



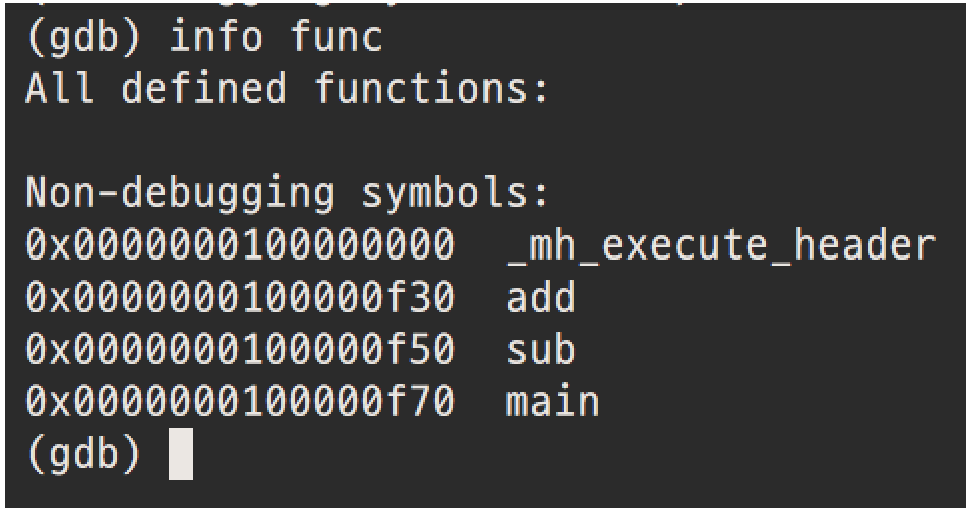
```
ta@canis01:~$ gdb bomb
GNU gdb (Ubuntu 7.7.1-0ubuntu5~14.04.3) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent 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 bomb...done.
(gdb) 
```

Tools - GDB

- Show functions: i(nfo) f(unc)



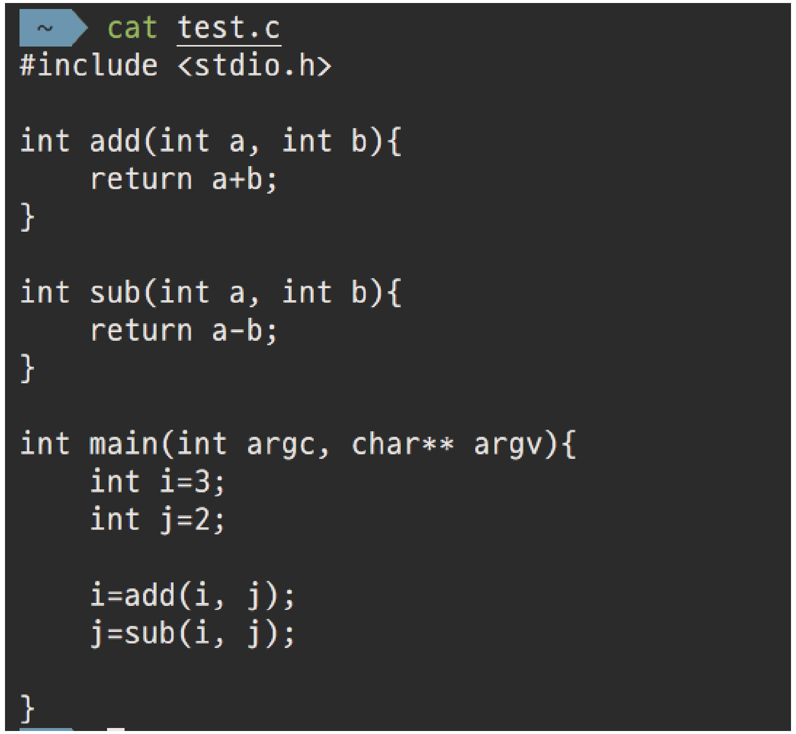
```
~  cat test.c
#include <stdio.h>

int add(int a, int b){
    return a+b;
}

int sub(int a, int b){
    return a-b;
}

int main(int argc, char** argv){
    int i=3;
    int j=2;

    i=add(i, j);
    j=sub(i, j);

}
```



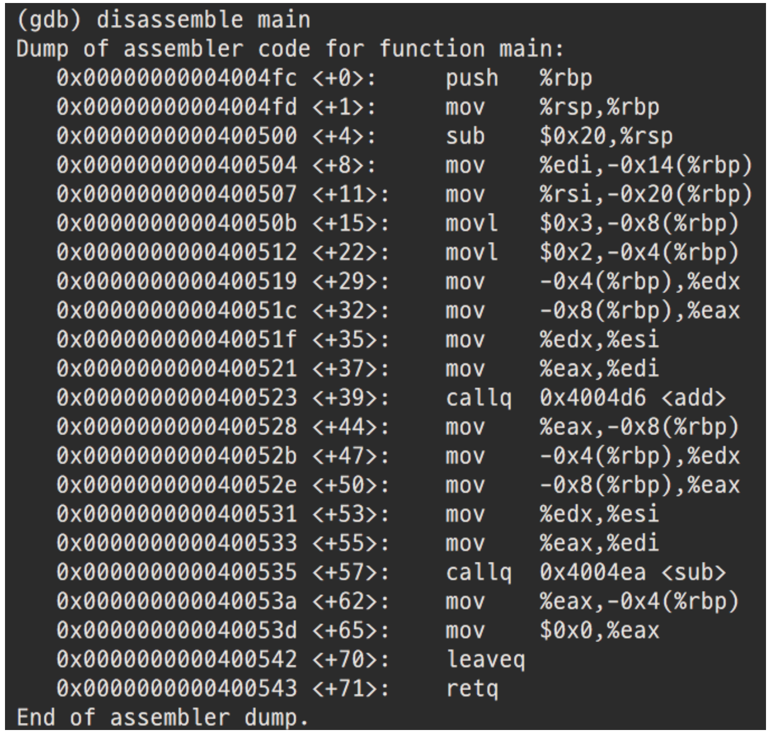
```
(gdb) info func
All defined functions:

Non-debugging symbols:
0x0000000100000000  _mh_execute_header
0x0000000100000f30  add
0x0000000100000f50  sub
0x0000000100000f70  main
(gdb) 
```

Tools - GDB

- View assembly of a function:
  disas(semble) [function name]



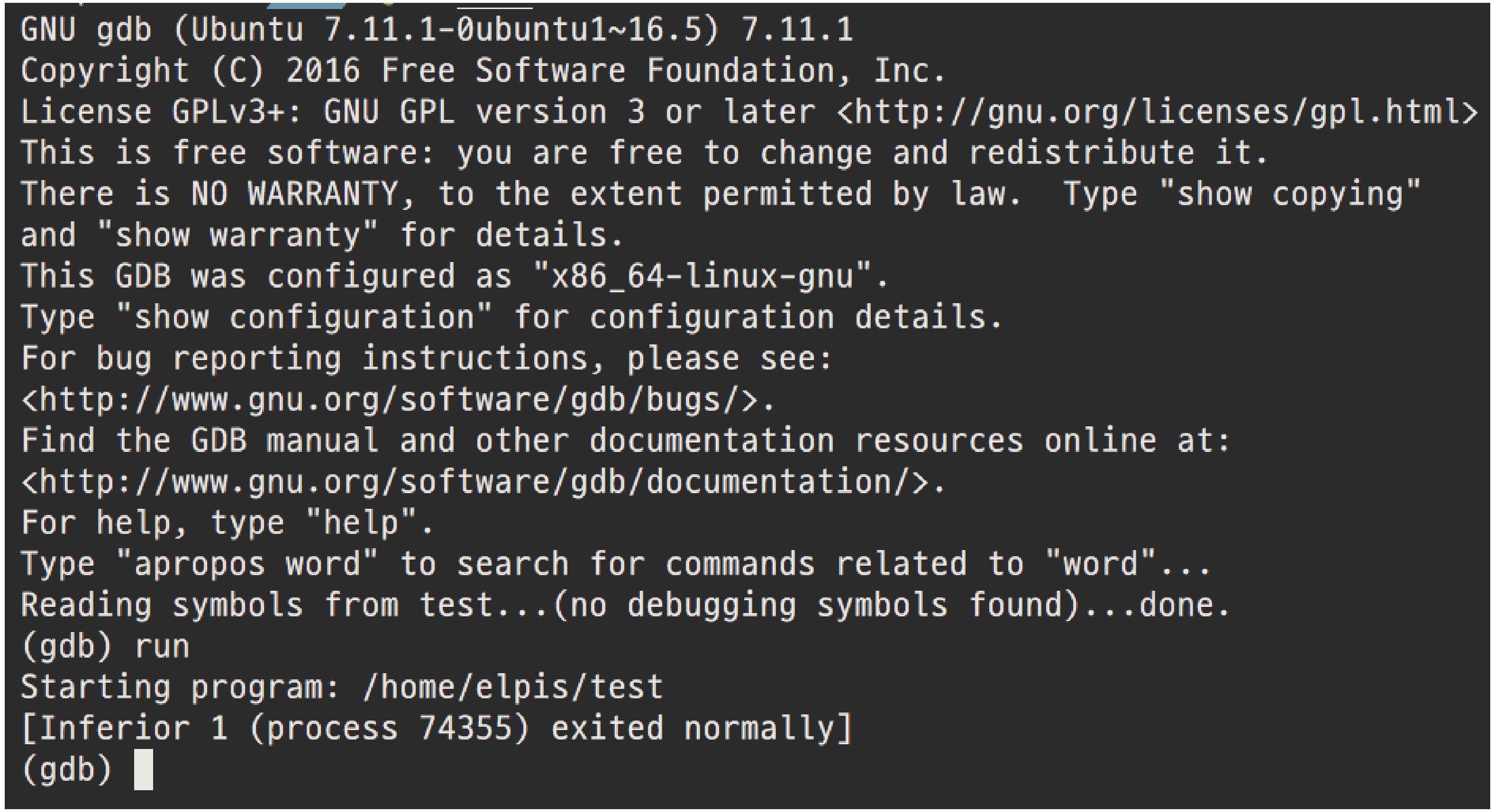
```
~  cat test.c
#include <stdio.h>

int add(int a, int b){
    return a+b;
}

int sub(int a, int b){
    return a-b;
}

int main(int argc, char** argv){
    int i=3;
    int j=2;

    i=add(i, j);
    j=sub(i, j);

}
```



```
(gdb) disassemble main
Dump of assembler code for function main:
   0x00000000004004fc <+0>:     push   %rbp
   0x00000000004004fd <+1>:     mov    %rsp,%rbp
   0x0000000000400500 <+4>:     sub    $0x20,%rsp
   0x0000000000400504 <+8>:     mov    %edi,-0x14(%rbp)
   0x0000000000400507 <+11>:    mov    %rsi,-0x20(%rbp)
   0x000000000040050b <+15>:    movl   $0x3,-0x8(%rbp)
   0x0000000000400512 <+22>:    movl   $0x2,-0x4(%rbp)
   0x0000000000400519 <+29>:    mov    -0x4(%rbp),%edx
   0x000000000040051c <+32>:    mov    -0x8(%rbp),%eax
   0x000000000040051f <+35>:    mov    %edx,%esi
   0x0000000000400521 <+37>:    mov    %eax,%edi
   0x0000000000400523 <+39>:    callq  0x4004d6 <add>
   0x0000000000400528 <+44>:    mov    %eax,-0x8(%rbp)
   0x000000000040052b <+47>:    mov    -0x4(%rbp),%edx
   0x000000000040052e <+50>:    mov    -0x8(%rbp),%eax
   0x0000000000400531 <+53>:    mov    %edx,%esi
   0x0000000000400533 <+55>:    mov    %eax,%edi
   0x0000000000400535 <+57>:    callq  0x4004ea <sub>
   0x000000000040053a <+62>:    mov    %eax,-0x4(%rbp)
   0x000000000040053d <+65>:    mov    $0x0,%eax
   0x0000000000400542 <+70>:    leaveq
   0x0000000000400543 <+71>:    retq
End of assembler dump.
```

Tools - GDB

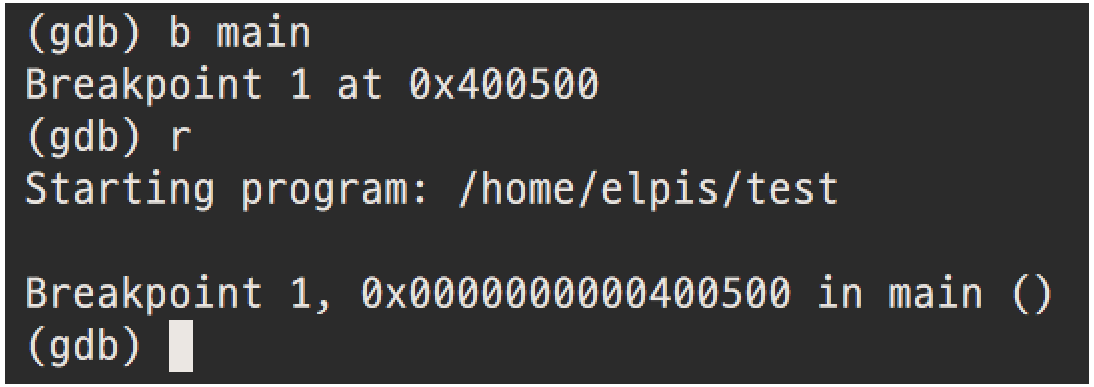
- Run program: r(un)



```
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 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 test...(no debugging symbols found)...done.
(gdb) run
Starting program: /home/elpis/test
[Inferior 1 (process 74355) exited normally]
(gdb)
```

Tools - GDB

- Breakpoints: Makes program to stop at certain point
  - b(reak) [line number]
  - b(reak) [function name]
  - b(reak) [file name]:[line number]
  - b(reak) *[address]



```
(gdb) b main
Breakpoint 1 at 0x400500
(gdb) r
Starting program: /home/elpis/test

Breakpoint 1, 0x0000000000400500 in main ()
(gdb)
```

Tools - GDB

- List current breakpoints: i(nfo) b(reakpoint)
- Disable breakpoint: disable [breakpoint number]
- Delete breakpoint: d(elete) [breakpoint number]
- Execute until breakpoint(or end of file): c(ontinue)
- Execute next instruction: n(ext)i

Tools - GDB

- For more details,
  - https://www.youtube.com/watch?v=svG6OPyKsrw
  - https://www.youtube.com/watch?v=sCtY--xRUyI

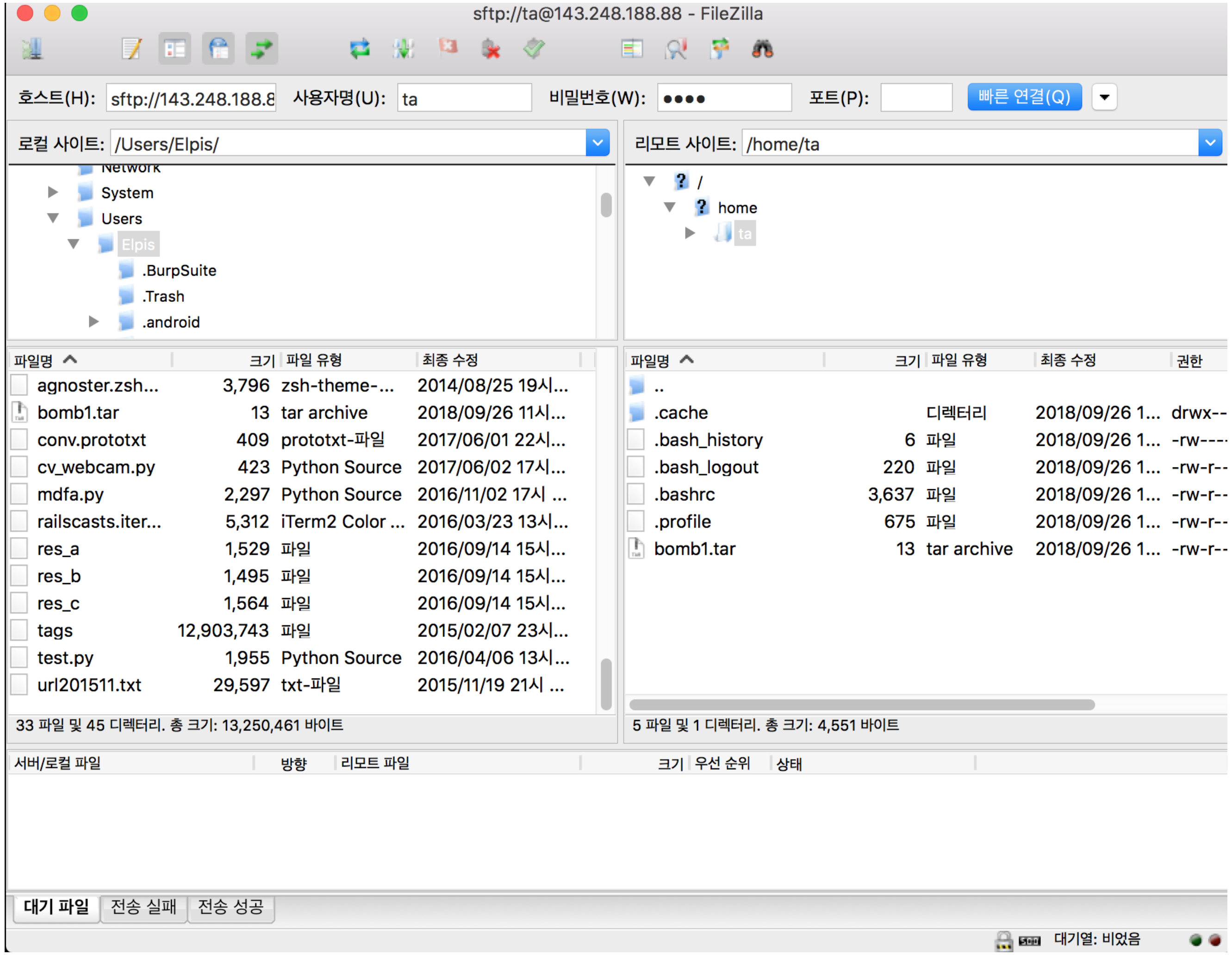
Tools – File transfer to server

- Copy a file from a machine to another
- WinSCP, FileZilla: for Windows (FileZilla is also for Mac/Linux)
  - User-friendly interface
- SCP: for Mac/Linux
  - built-in commands in the shell

- **Don’t forget to turn on your KVPN**

Download links: FileZilla - https://filezilla-project.org/
WinSCP - https://winscp.net/eng/download.php

Example: FileZilla



sftp://ta@143.248.188.88 - FileZilla

호스트(H): sftp://143.248.188.8 사용자명(U): ta 비밀번호(W): ●●●● 포트(P):

로컬 사이트: /Users/Elpis/

리모트 사이트: /home/ta

파일명	크기	파일 유형	최종 수정
agnoster.zsh...	3,796	zsh-theme-...	2014/08/25 19시...
bomb1.tar	13	tar archive	2018/09/26 11시...
conv.prototxt	409	prototxt-파일	2017/06/01 22시...
cv_webcam.py	423	Python Source	2017/06/02 17시...
mdfa.py	2,297	Python Source	2016/11/02 17시 ...
railscasts.iter...	5,312	iTerm2 Color ...	2016/03/23 13시...
res_a	1,529	파일	2016/09/14 15시...
res_b	1,495	파일	2016/09/14 15시...
res_c	1,564	파일	2016/09/14 15시...
tags	12,903,743	파일	2015/02/07 23시...
test.py	1,955	Python Source	2016/04/06 13시...
url201511.txt	29,597	txt-파일	2015/11/19 21시 ...

33 파일 및 45 디렉터리. 총 크기: 13,250,461 바이트

파일명	크기	파일 유형	최종 수정	권한
..				
.cache		디렉터리	2018/09/26 1...	drwx--
.bash_history	6	파일	2018/09/26 1...	-rw----
.bash_logout	220	파일	2018/09/26 1...	-rw-r--
.bashrc	3,637	파일	2018/09/26 1...	-rw-r--
.profile	675	파일	2018/09/26 1...	-rw-r--
bomb1.tar	13	tar archive	2018/09/26 1...	-rw-r--

5 파일 및 1 디렉터리. 총 크기: 4,551 바이트

서버/로컬 파일	방향	리모트 파일	크기	우선 순위	상태

SCP Commands

- Execute as following on shell:

> scp [target file location] [username]@[server IP]:[destination(directory)]

- Example: scp bomb1.tar ta@143.248.188.188:~

  - Move **bomb1.tar** from local machine's current directory to home directory(**~**) of account **ta** in **143.248.188.188**

Precautions

- You’d better **not work** with multiple bombs
  - Explosion signal from every bomb will be reported
- You must download bomb **using your information**
  - Using other’s information will be considered as cheating
- You should run your binary bomb on **class machine**
  - If not, the bomb will refuse to run.
- This is an **individual project**

Hints

- You may prevent explosion by using GDB breakpoint
  - Note that breakpoints are volatile
- Secret phase
  - For more challenge, you can find out secret phase.
- All bombs are different
  - So, do not try your friend's answer on your bomb ☺

FAQs

- Permission denied error
  - Use chmod command to change permission
  - Cannot execute: chmod +x
  - Cannot read: chmod +r
  - Cannot wrote: chmod +w

- Invalid host error
  - Work on the class server

- FileZilla connection failure
  - Don't forget the KVPN