

**IE4012**

**Offensive Hacking: Tactical and Strategic**

**4th Year, 1st Semester**

Lab Report

**BIG BANG THEORY**

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

29/03/2020

**Declaration**

I certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of my knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

Registration Number: IT17108546

Name: Jayawardhana D D T

**Table of Contents**

[1. Solutions to Sheldon1 3](#_Toc36392670)

[Sheldon1 Phase 1 3](#_Toc36392671)

# Solutions to Sheldon1

## Sheldon1 Phase 1

To do this exercise, I am using a machine with running Ubuntu. First, you need to download the repository from GitHub and unzip the file in a directory you like. Then make sure you make the file ‘sheldon1’ executable before running it on a debugger.

*Note: Since ‘sheldon1’ is a 32bit ELF file, if you run into any errors when using gdb debugger that fails to run the file, use the command below to install the necessary dependencies before proceeding with the debugging.*

**sudo apt-get install libc6:i386**

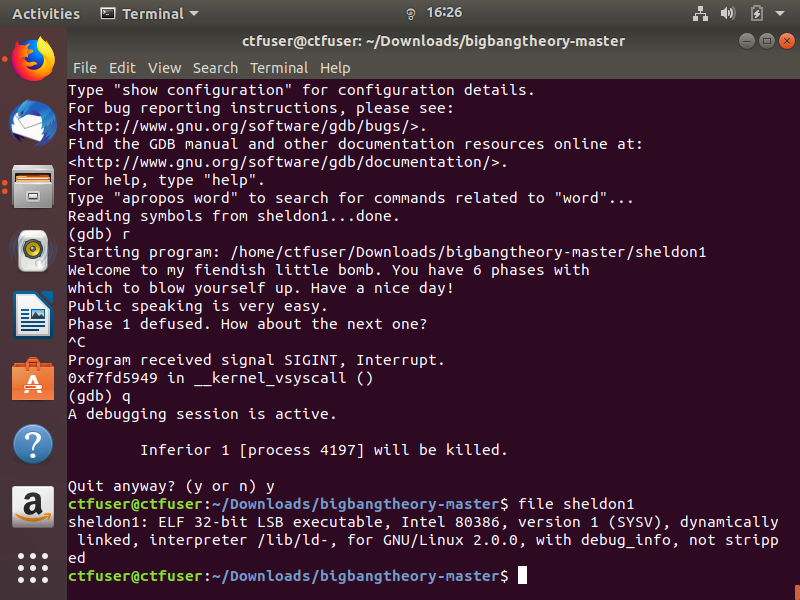
****

Figure .: Identify File Type

When everything is set, to start debugging, first run the following command.

**strings sheldon1**

The strings command returns all the string values in a file. Hence, we can look for any odd sentences or words that could be the key to unlocking phase 1.

As shown in the Figure 1.2, the strings command lists a huge amount of words and sentences from the file ‘sheldon1’. From these sentences and words, it could be noted that the following stands out.

**Public speaking is very easy.**

Now that we have a potential key for unlocking phase 1, we can start the debugging. To do so, we need to run the following command to open the GDB debugger.

**gdb sheldon1**

Now you can see that we are inside the debugger in file ‘sheldon1’. To run the file, use the following command.

**run** or **r**

After running the command, we will be greeted with a welcome message. Here you can copy and paste the sentence we found earlier i.e. “Public speaking is very easy.”. Make sure to include the period at the end too. Now press ‘Enter’.

The resulting message says that we have successfully difused phase 1.

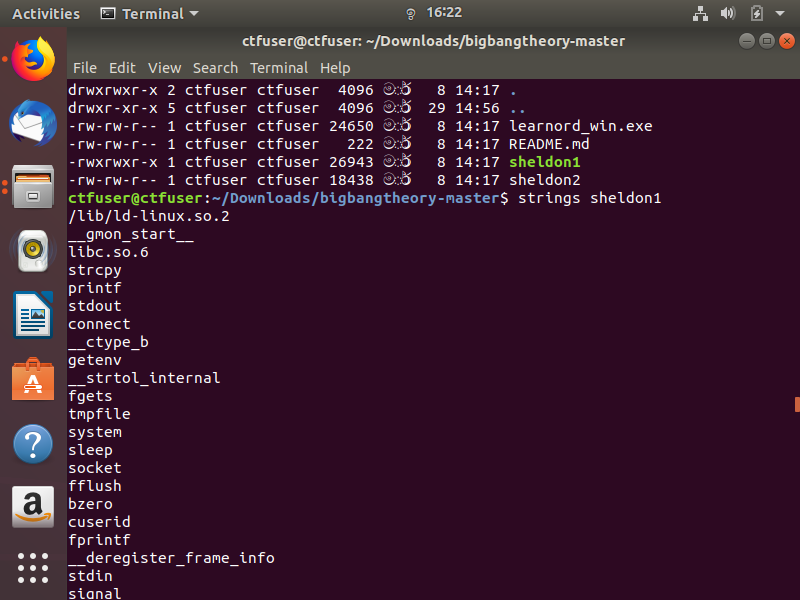
****

Figure .: Using the Stings Command

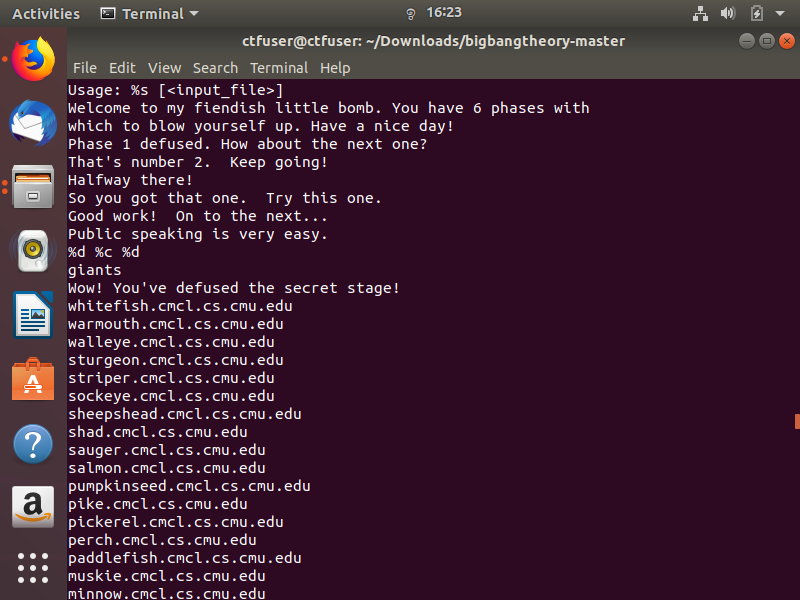
****

Figure .: Identifying the Probable Sentence

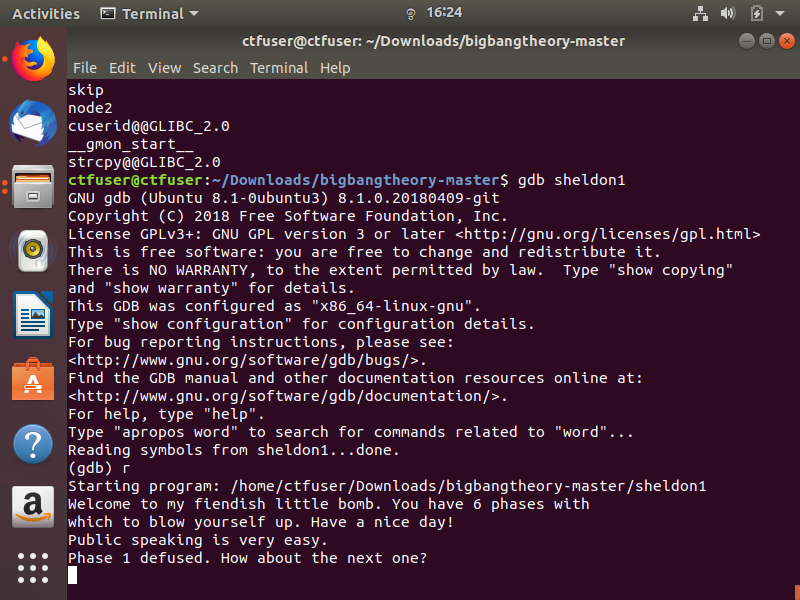
****

Figure .: Defusing Phase 1 with GDB