# CIT 430-530: Forensic Activity #1.2 – SIFT Access

Complete the following task in your SIFT workstation. Insert screenshots directly into this document where indicated and be sure they are legible.

## Tasks:

1. Boot SIFT and select the default useraccount **SANS Forensics**
2. Use the password: **forensics**
3. A new terminal window should automatically open, but if it does not, select the terminal icon in the left menu bar.



1. Issue the following commands and screenshot your results below:

**id**

**who**

**A screenshot of a computer

Description automatically generated with medium confidence**

1. Change to the Downloads directory and provide a screenshot of the files in the directory.
   1. *Note: you do not need to provide the files contained in the subdirectories*.   
      Graphical user interface, text

      Description automatically generated
2. Change to the home directory

**cd ~**

1. Start a ssh session to the following device. Include a screenshot of the new prompt if your ssh was successful including the timestamp information.
   1. Accept any RSA key messages by typing ‘yes’ without the quotes
   2. Use a password of ‘cit247’ without the quotes

**ssh** [**student@10.2.56.15**](mailto:student@10.2.56.15)

**Text

Description automatically generated**

1. Close the ssh session by typing ‘exit’ and minimize your terminal.
2. How many documents are listed on your SIFT Desktop?
   1. 16
3. Verify this amount using the terminal. Screenshot your terminal output below, including the commands used to find this information.
4. Cd Desktop, ls | wc -l
   1. Text

      Description automatically generated
5. From your prompt change to root using the command below, then change back to the regular sansforensics account. Screenshot your commands.
   1. Note your final prompt should not have the word ‘root’ in it.

**sudo su –**

Text

Description automatically generated

Type exit to exit the root user

## Submission

**Submit a completed copy of this document to Canvas by the due date.**