Steganography

Cyber Discovery 2.0

Investigative Session Day 3

Steganography

- Steganography
  - From the Greek word steganos meaning “covered”
  - And the Greek word graphie meaning “writing”

- Steganography is the process of hiding of a secret message within an ordinary message and extracting it at its destination

- Anyone else viewing the message will fail to know it contains hidden/encrypted data

Examples in History

- Greek history – Warning of an invasion, write message on tablet, then cover it in wax and write a fake message on top of wax. Or don't put anything on wax and it will appear to be blank.
- Tattoos on shaved heads - Shave head, tattoo message, then grow hair back. Upon transmission, shaving again will reveal message
- Both Axis and Allied spies during World War II used such measures as invisible inks
  - Using milk or fruit juice which darken when heated.
- WWII: Navaho code talkers - no real "code"; just a language unknown to the Japanese
- Messages written on envelopes in the area covered by postage stamps.

Null Cipher

- Null Ciphers:
  - Mix plaintext with large amount of fake data
- Example
- PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.
- 1st letter of each word gives message

  PERSHING SAILS FROM NY JUNE I

Null Cipher

- Another example
- In**s**pector number five de**t**aches the new fo**r**ms found with th**i**s shipment. Stop. Ac**k**nowledge earliest opportunity th**e** first new co**n**tract you receive fr**o**m their courier Ho**w**ton. Stop.

- 3rd letter of every 3rd word gives:

  strike now

Null Cipher

- Now it’s your turn:

- I**t**’s Thursday. T**h**at means w**e** need S**k**yler to g**e**t to S**y**lvia’s house, p**i**ck up O**s**car, and a**c**t casual. T**h**at way w**e** can t**r**uly see h**i**m surprised t**o**night.

- 2nd letter of every 2nd word gives:

  the key is cherio

Steganography

- Modern digital Steganography
  - Data is inserted and hidden, using a special algorithm, which may add and/or modify the contents of the file
  - This technique may simply append the data to the file, or disperse it throughout
  - Carefully crafted programs apply the data such that patterns appear normal.

Steganography

- Steganography Carrier Files
  - Digital images (bmp, gif, jpeg)
  - Audio files (mp3, wav)

- These are the most widely used medium being used today

Steganography

- Almost anything can be hidden in digital data
  - MS Word (doc)
  - Web pages (htm)
  - Executables (exe)
  - Audio files (mp3, wav, cda)
  - Video files (mpeg, avi)
  - Digital images (bmp, gif, jpg)

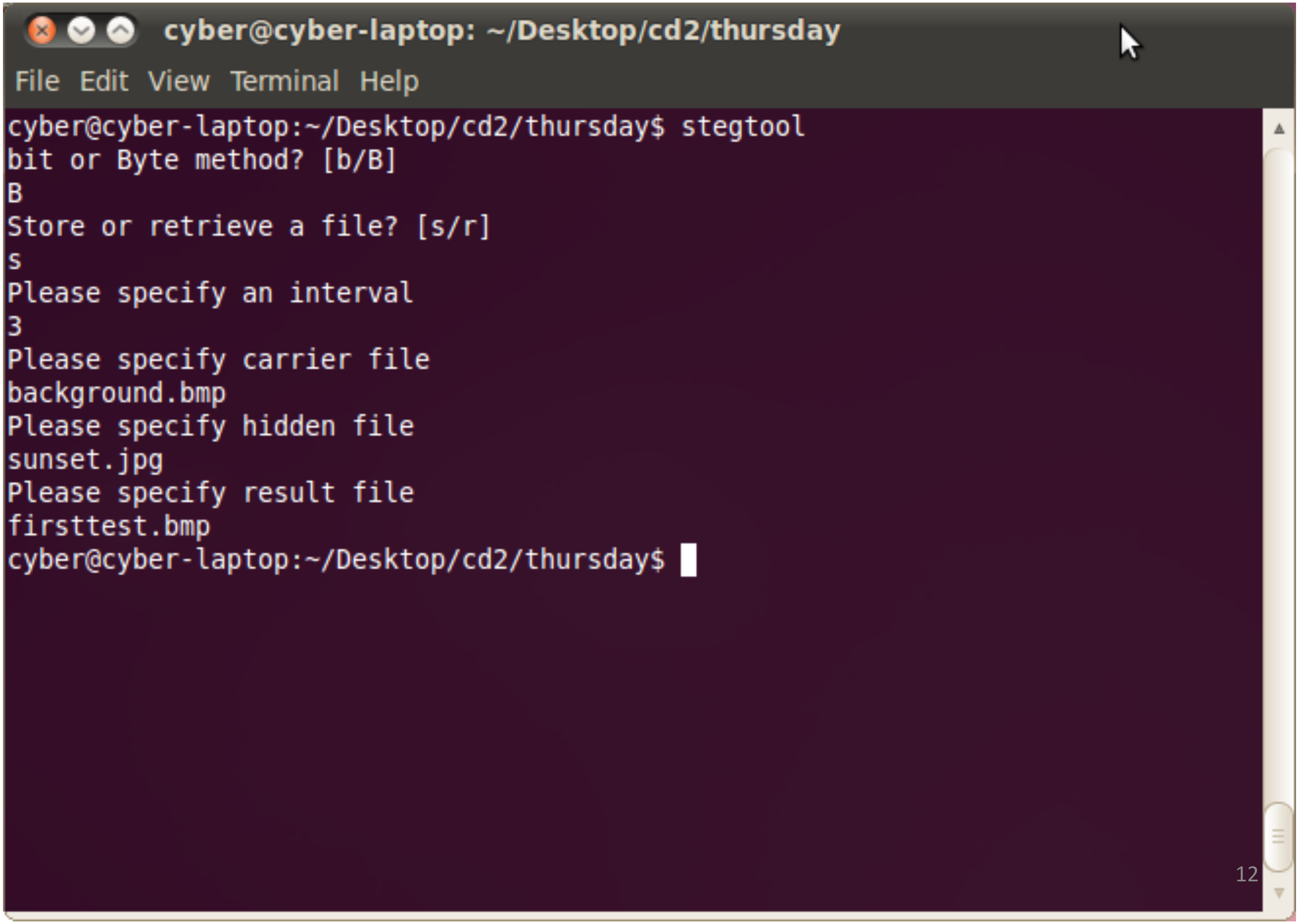
Steganography

- Methods for Bitmap
  - Bitmaps use Red, Green, and Blue values (8 bits each) for every pixel
  - Replace last bit (or two), known as the least significant bit, of each RGB value with bit(s) from the secret message
  - Or replace every nth pixel with value of message
- Why do you think this will work?
  - Takes advantage of our limited visual perception of colors

Hands-on

- Let’s try to insert and extract from a few files
- We’ll be using the `stegtool` applications

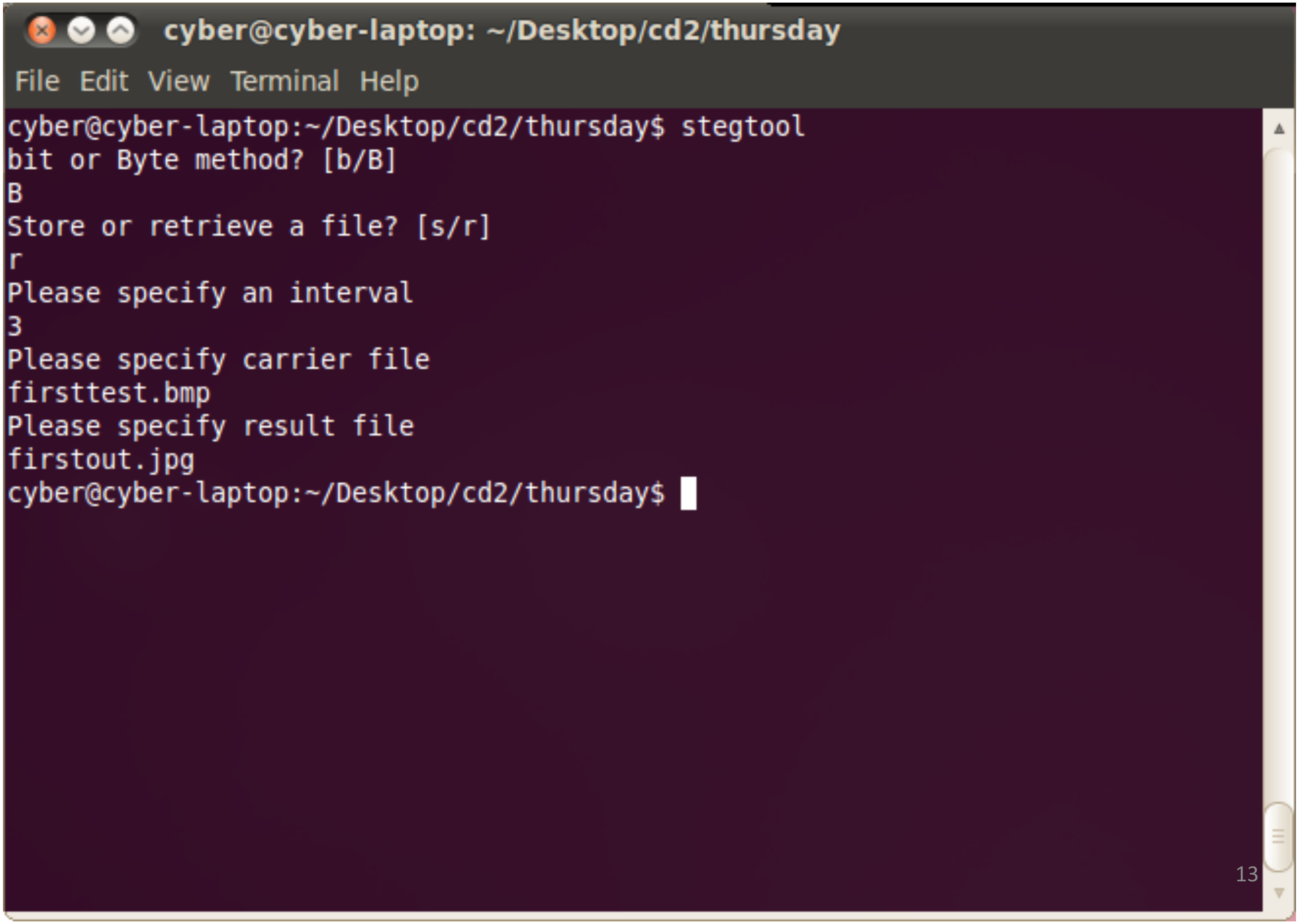
Store – Byte method



cyber@cyber-laptop: ~/Desktop/cd2/thursday
File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/thursday$ stegtool
bit or Byte method? [b/B]
B
Store or retrieve a file? [s/r]
s
Please specify an interval
3
Please specify carrier file
background.bmp
Please specify hidden file
sunset.jpg
Please specify result file
firsttest.bmp
cyber@cyber-laptop:~/Desktop/cd2/thursday$
```

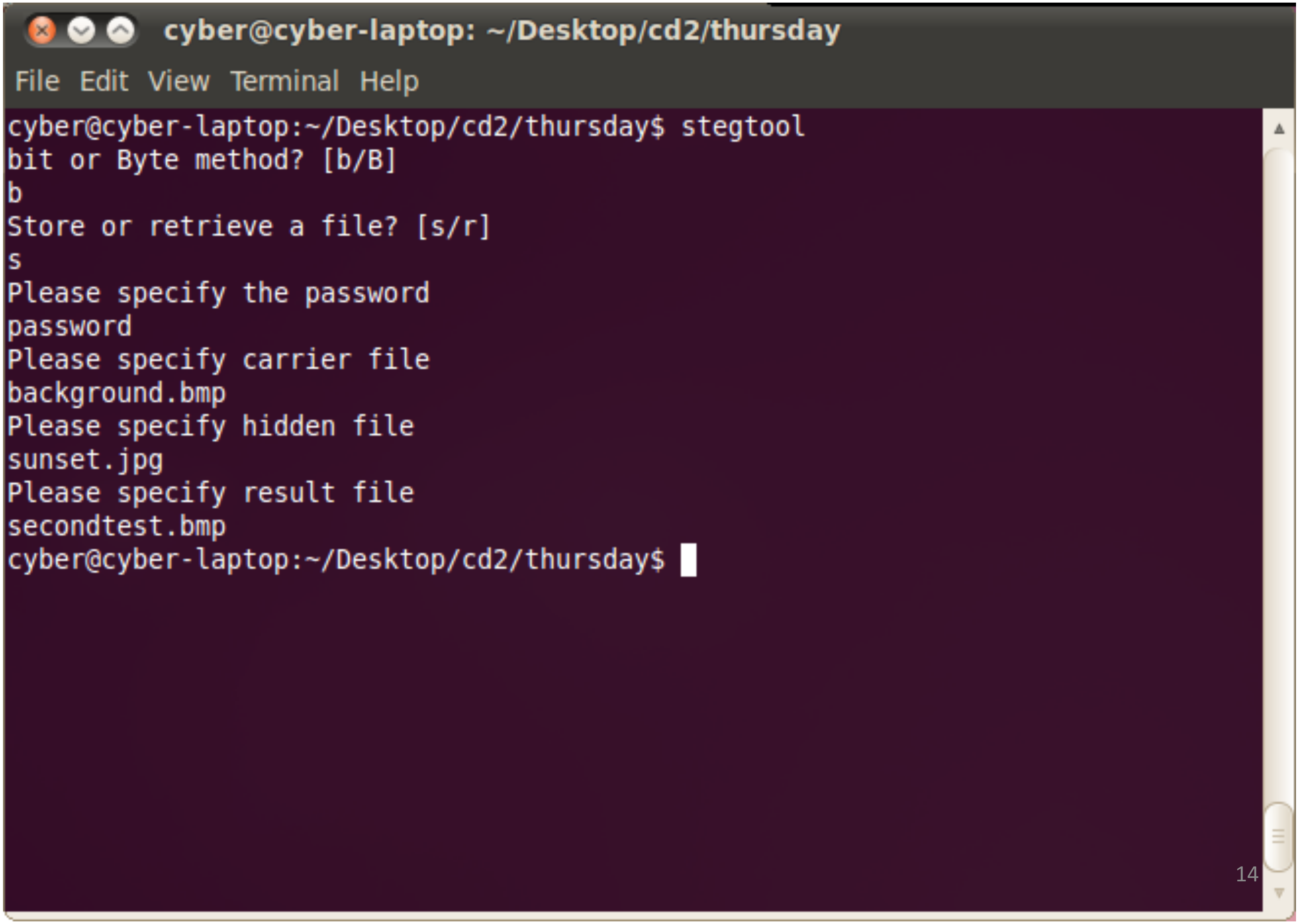
Retrieve – Byte method



cyber@cyber-laptop: ~/Desktop/cd2/thursday
File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/thursday$ stegtool
bit or Byte method? [b/B]
B
Store or retrieve a file? [s/r]
r
Please specify an interval
3
Please specify carrier file
firsttest.bmp
Please specify result file
firstout.jpg
cyber@cyber-laptop:~/Desktop/cd2/thursday$ 
```

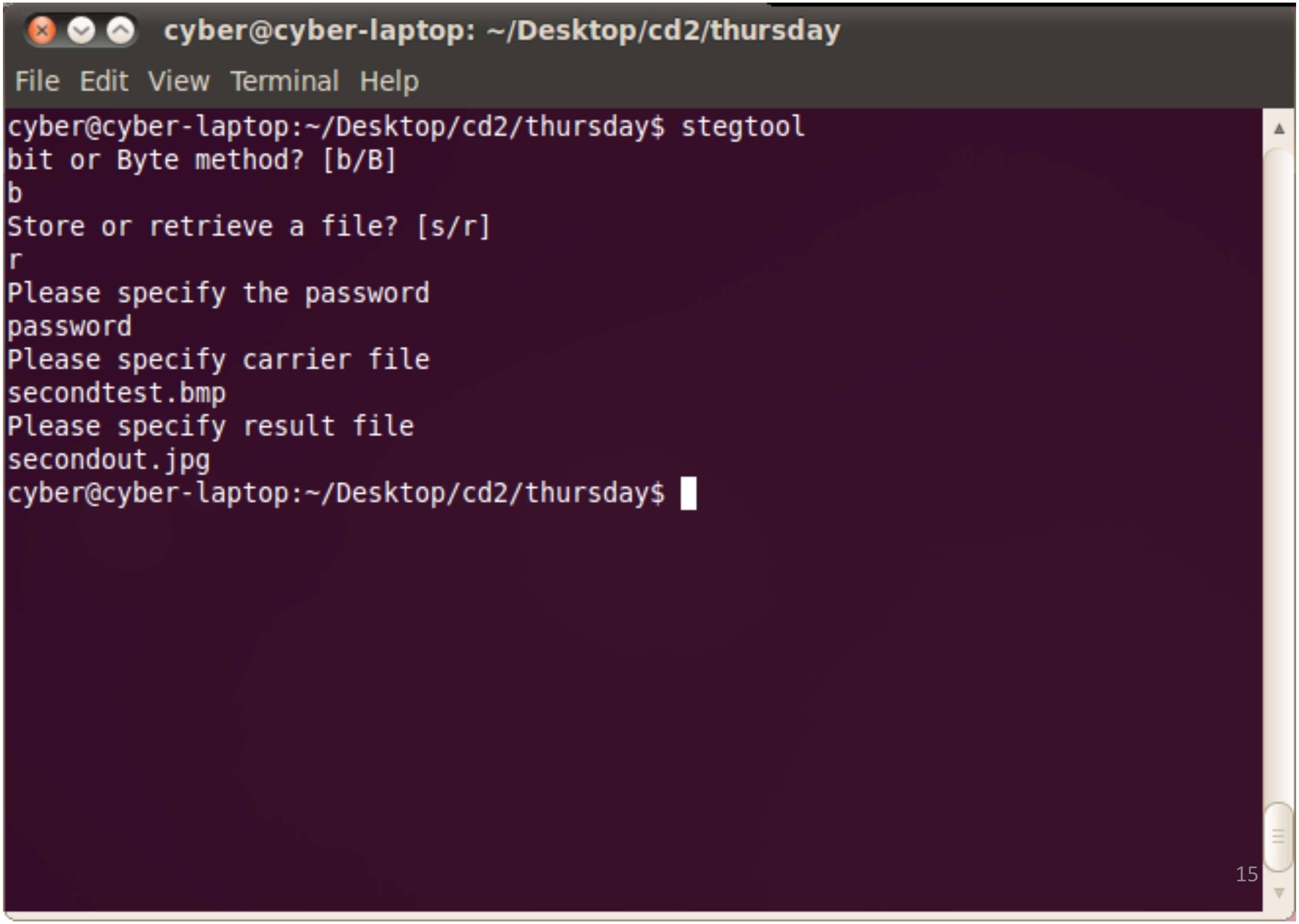
Store – Bit method



cyber@cyber-laptop: ~/Desktop/cd2/thursday
File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/thursday$ stegtool
bit or Byte method? [b/B]
b
Store or retrieve a file? [s/r]
s
Please specify the password
password
Please specify carrier file
background.bmp
Please specify hidden file
sunset.jpg
Please specify result file
secondtest.bmp
cyber@cyber-laptop:~/Desktop/cd2/thursday$ 
```

Retrieve – Bit method



cyber@cyber-laptop: ~/Desktop/cd2/thursday
File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/thursday$ stegtool
bit or Byte method? [b/B]
b
Store or retrieve a file? [s/r]
r
Please specify the password
password
Please specify carrier file
secondtest.bmp
Please specify result file
secondout.jpg
cyber@cyber-laptop:~/Desktop/cd2/thursday$ 
```

Steganography

- Your turn to try to insert and extract a file.

- Carrier Files
  - background.bmp
  - mountain.bmp
  - trees.bmp
- Hidden Files
  - sunset.jpg
  - turtle.jpg

- Use `stegtool` to insert and extract files