

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
- **P**RESIDENT'S **E**MBARGO **R**ULING **S**HOULD **H**AVE
IMMEDIATE **N**OTICE. **G**RAVE **S**ITUATION **A**FFECTING
INTERNATIONAL **L**AW. **S**TATEMENT **F**ORESHADOWS
RUIN **O**F **M**ANY **N**EUTRALS. **Y**ELLOW **J**OURNALS
UNIFYING **N**ATIONAL **E**XCITEMENT **I**MMENSELY.
- 1st letter of each word gives message
PERSHING SAILS FROM NY JUNE I

Null Cipher

- Another example
- Insspector number five dettaches the new forrms found with this shipment. Stop. Ackknowledge earliest opportunity the first new conntract you receive from their courier Howton. Stop.
- 3rd letter of every 3rd word gives:
strike now

Null Cipher

- Now it's your turn:
- It's Thursday. That means we need Skyler to get to Sylvia's house, pick up Oscar, and act casual. That way we can truly see him surprised tonight.
- 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)

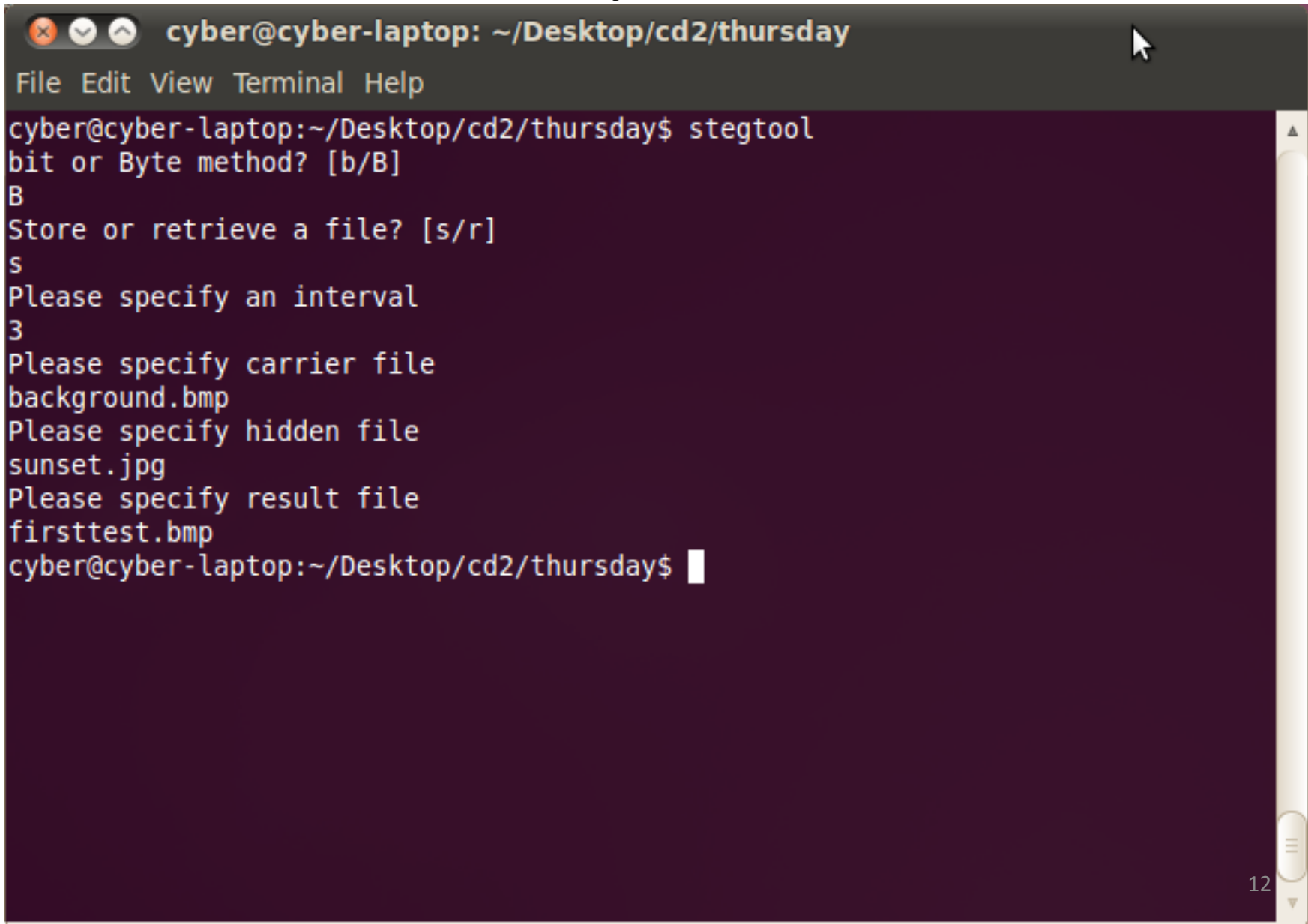
Steganography

- 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

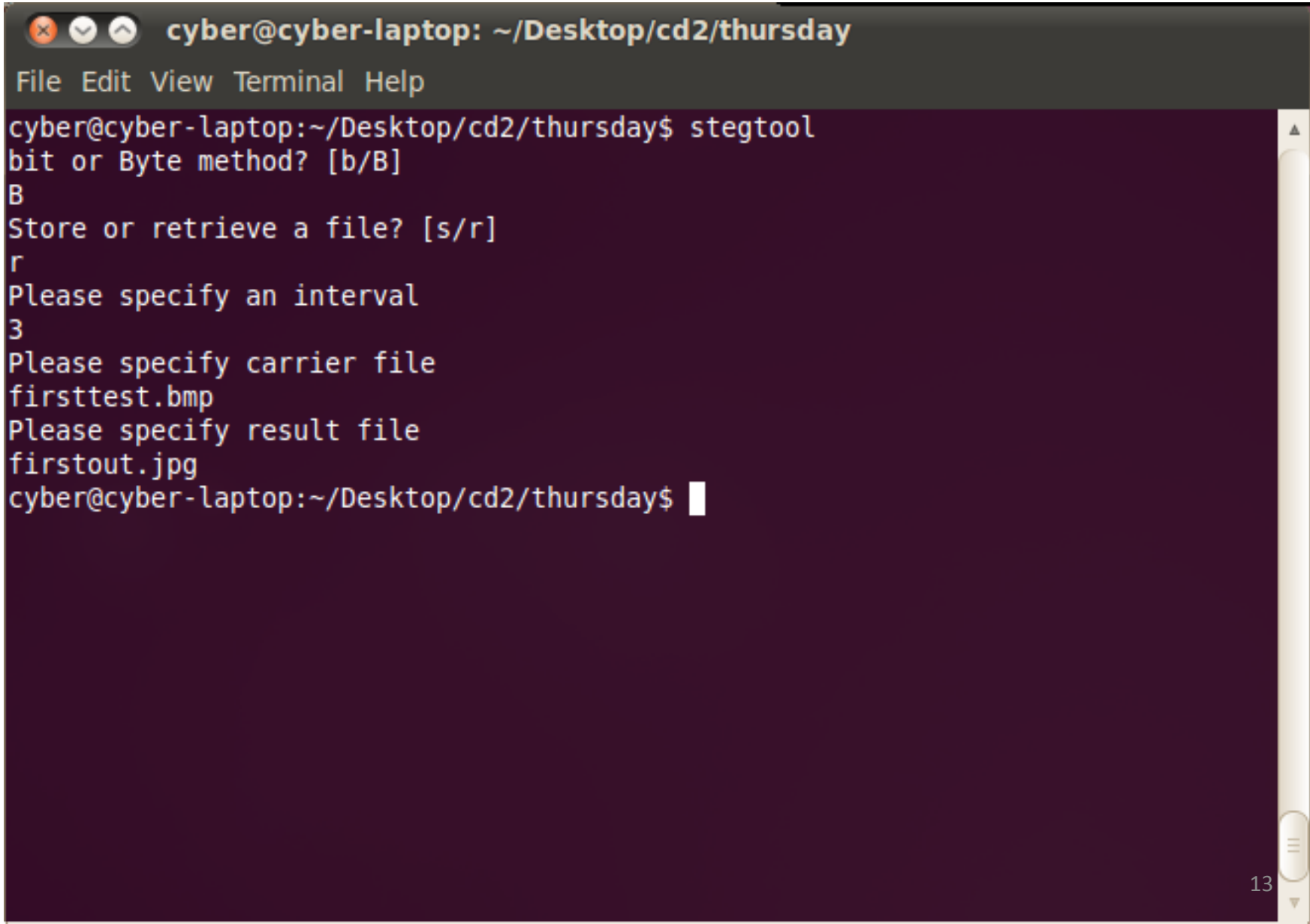
Store – Byte method



```
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$
```

The image shows a terminal window titled "cyber@cyber-laptop: ~/Desktop/cd2/thursday". The window has a menu bar with "File", "Edit", "View", "Terminal", and "Help". The terminal content shows the execution of the "stegtool" command. It prompts for "bit or Byte method?" with input "B", then "Store or retrieve a file?" with input "s". It then prompts for an interval (input "3"), a carrier file ("background.bmp"), a hidden file ("sunset.jpg"), and a result file ("firsttest.bmp"). The prompt "cyber@cyber-laptop:~/Desktop/cd2/thursday\$" is shown at the end with a cursor. A mouse cursor is visible in the top right corner of the terminal window. The terminal has a dark purple background and a vertical scrollbar on the right side.

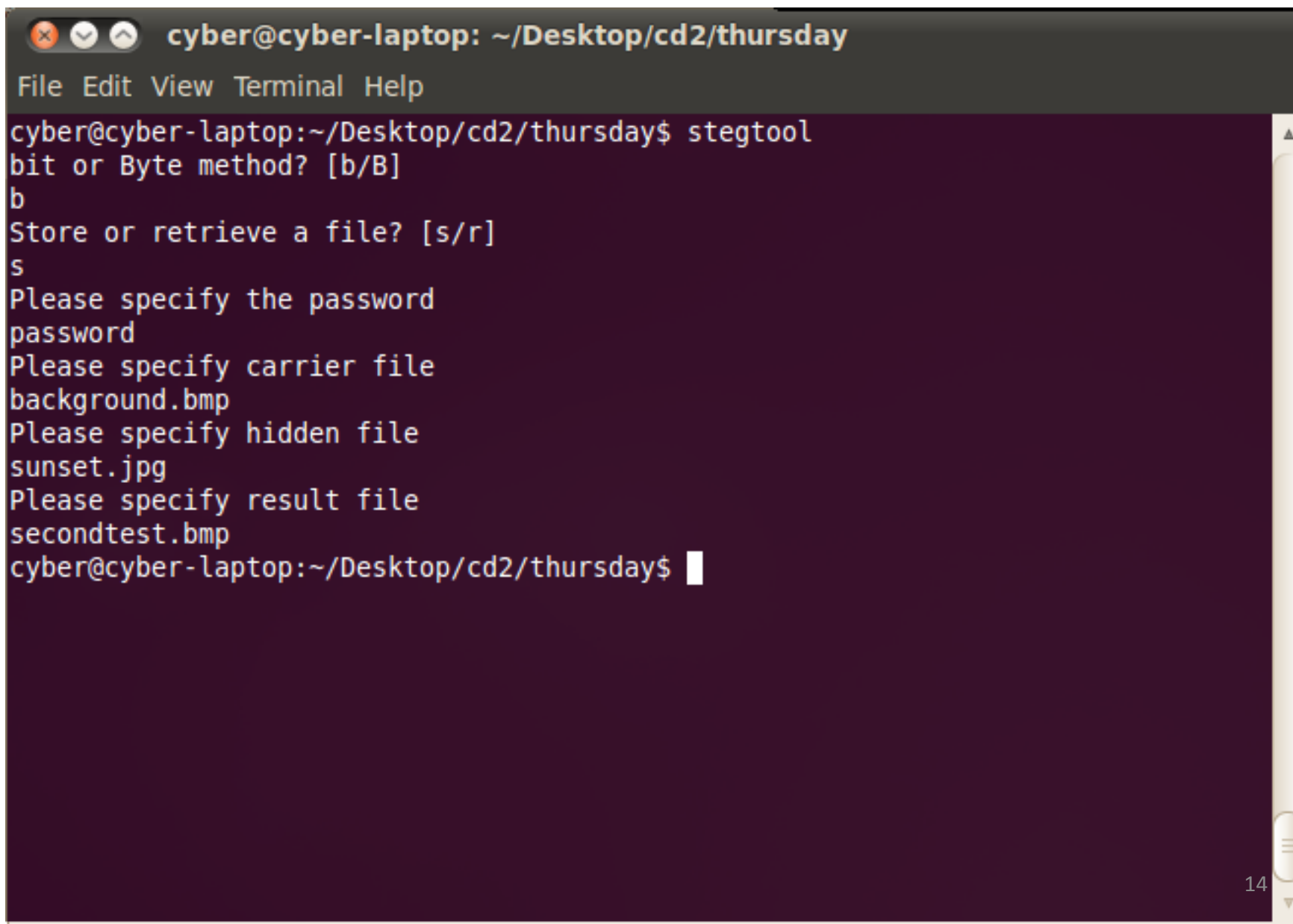
Retrieve – Byte method



```
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$
```

The image shows a terminal window titled "cyber@cyber-laptop: ~/Desktop/cd2/thursday". The window has a menu bar with "File", "Edit", "View", "Terminal", and "Help". The terminal content shows the execution of the "stegtool" command. It prompts for "bit or Byte method?" with options "[b/B]", where 'B' is entered. It then prompts for "Store or retrieve a file?" with options "[s/r]", where 'r' is entered. Next, it prompts for "Please specify an interval", where '3' is entered. Then, it prompts for "Please specify carrier file", where "firsttest.bmp" is entered. Finally, it prompts for "Please specify result file", where "firstout.jpg" is entered. The prompt "cyber@cyber-laptop:~/Desktop/cd2/thursday\$" is shown at the bottom with a cursor. The terminal has a dark purple background and a light-colored scrollbar on the right side.

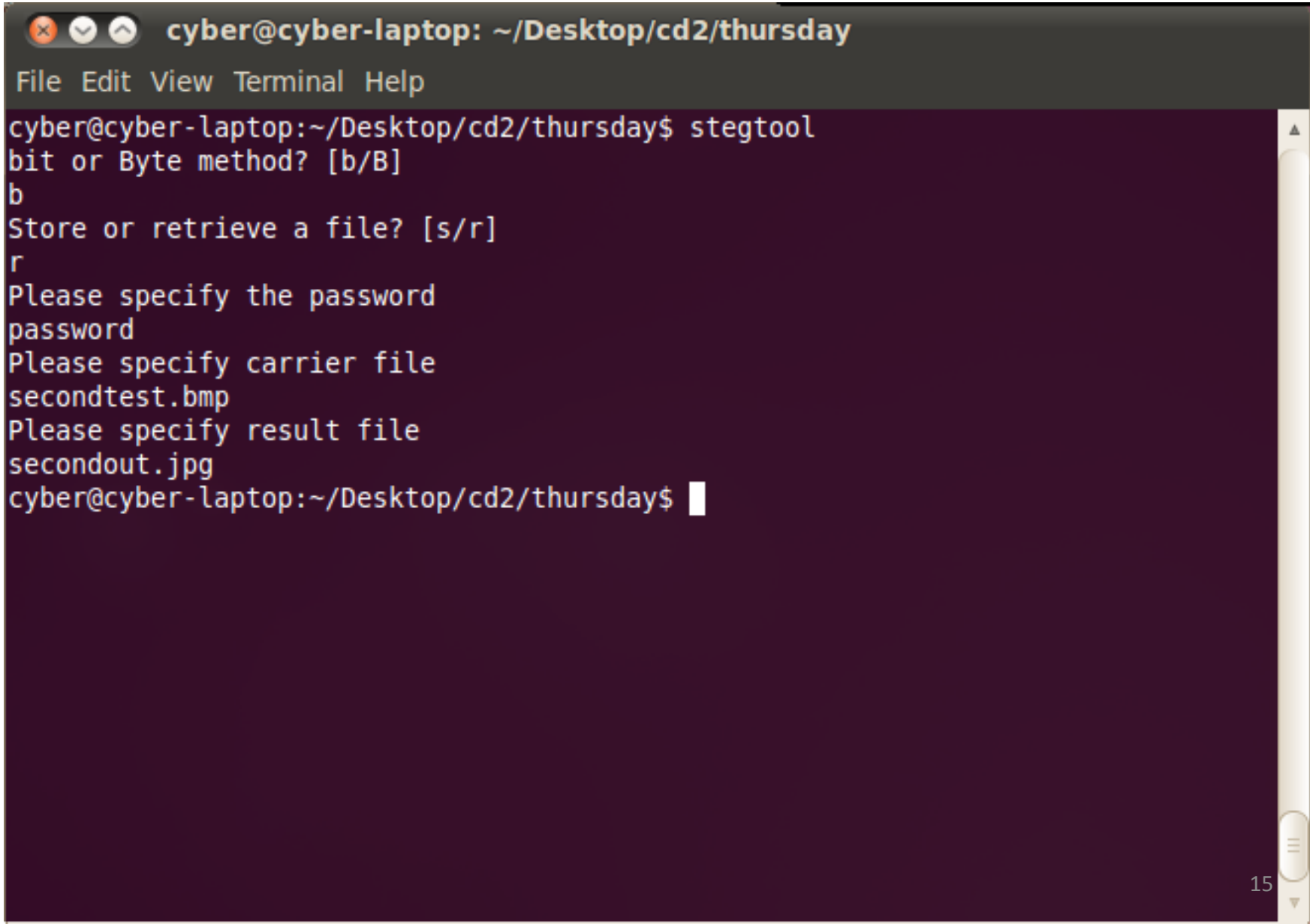
Store – Bit method



```
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$
```

The image shows a terminal window titled "cyber@cyber-laptop: ~/Desktop/cd2/thursday". The window has a menu bar with "File", "Edit", "View", "Terminal", and "Help". The terminal content shows the execution of the "stegtool" command. It prompts for a method ("bit or Byte method? [b/B]"), where 'b' is entered. It then asks "Store or retrieve a file? [s/r]", where 's' is entered. Subsequent prompts are for a password ("password"), a carrier file ("background.bmp"), a hidden file ("sunset.jpg"), and a result file ("secondtest.bmp"). The terminal ends with the prompt "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$
```

The image shows a terminal window titled "cyber@cyber-laptop: ~/Desktop/cd2/thursday". The window has a menu bar with "File", "Edit", "View", "Terminal", and "Help". The terminal content shows the execution of the "stegtool" command. The user is prompted to choose between "bit" and "Byte" methods, selects "b", then prompted to choose between "Store" and "retrieve" a file, selects "r", and then provides the password "password", the carrier file "secondtest.bmp", and the result file "secondout.jpg". The prompt returns to the shell.

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