

cyber discovery camp

SPONSORED BY
*Louisiana Tech University
and Cyber Innovation Center*



Cyber DISCOVERY

→ Steganography

INVESTIGATIVE SESSION 3

PowerBook G4

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
- Inspector number five detaches the new forms found with this shipment. Stop. Acknowledge earliest opportunity the first new contract 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 using his cart gather ebony and cedar for Trevor.
- 2nd letter of every 2nd word gives:
the key is saber



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
 - Word Processor (doc, docx, odt)
 - 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 Cyber Discovery Toolkit application





Computer



Home



Presentations



Menu ⌘ ⌘ ⌘ ⌘

PowerBook G4

👤 ⚡ 🔋 🔍 20:12 ☰



Computer



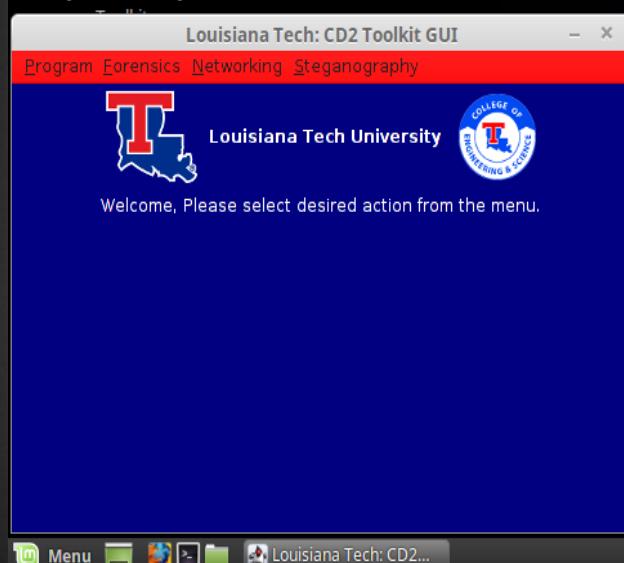
Home



Presentations



Cyber Discovery

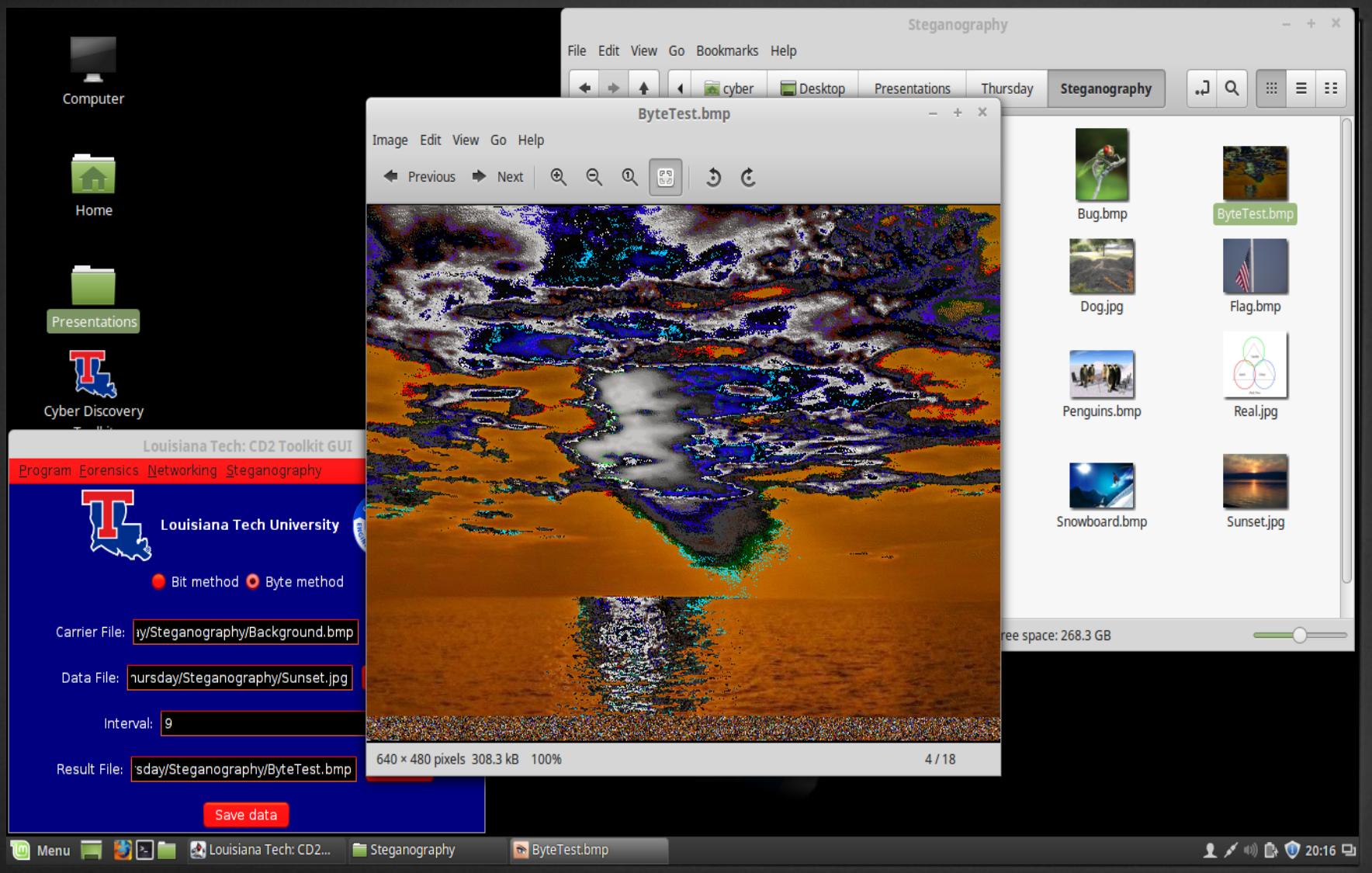


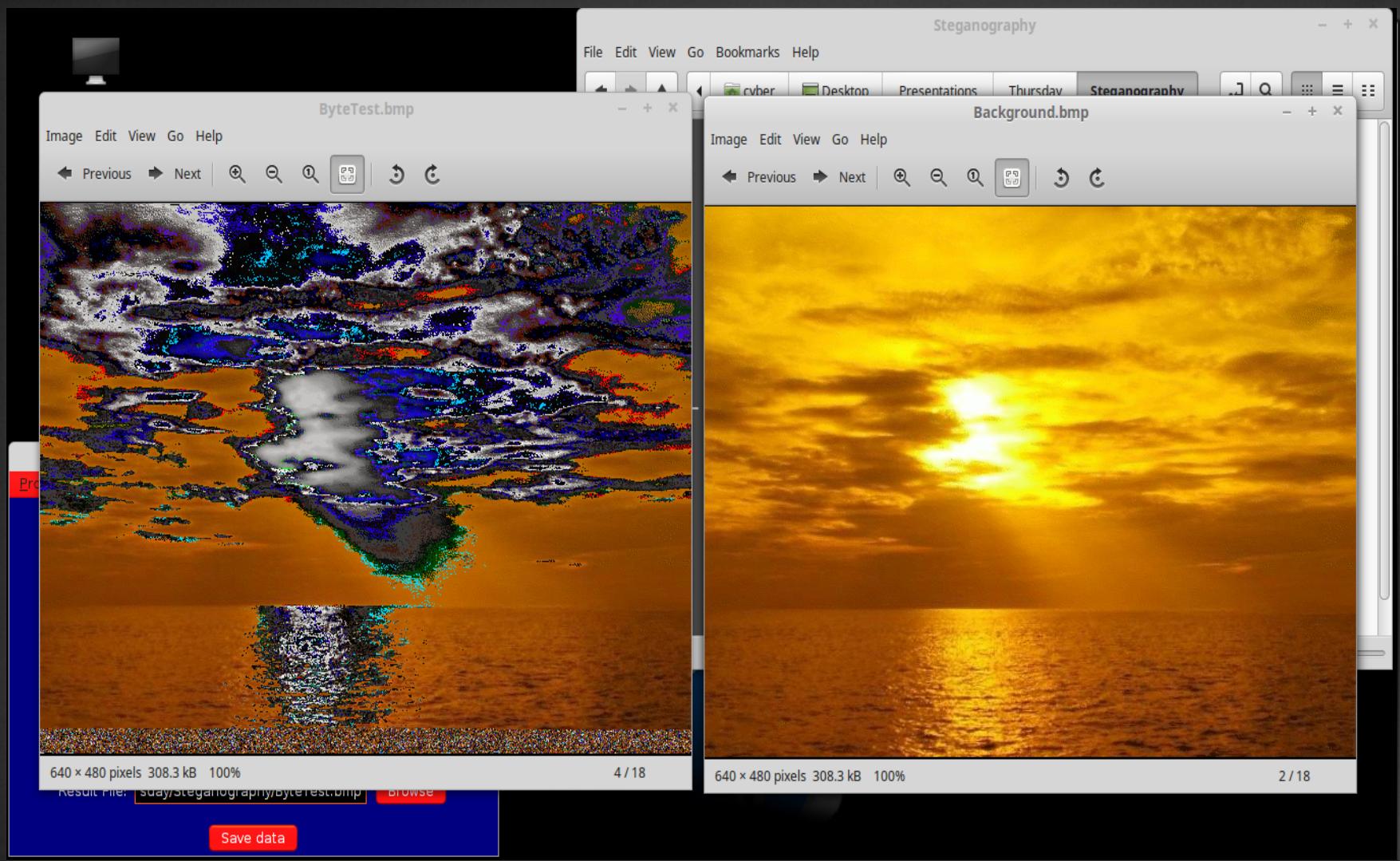
Menu File Edit Program Louisiana Tech: CD2... PowerBook G4 20:13







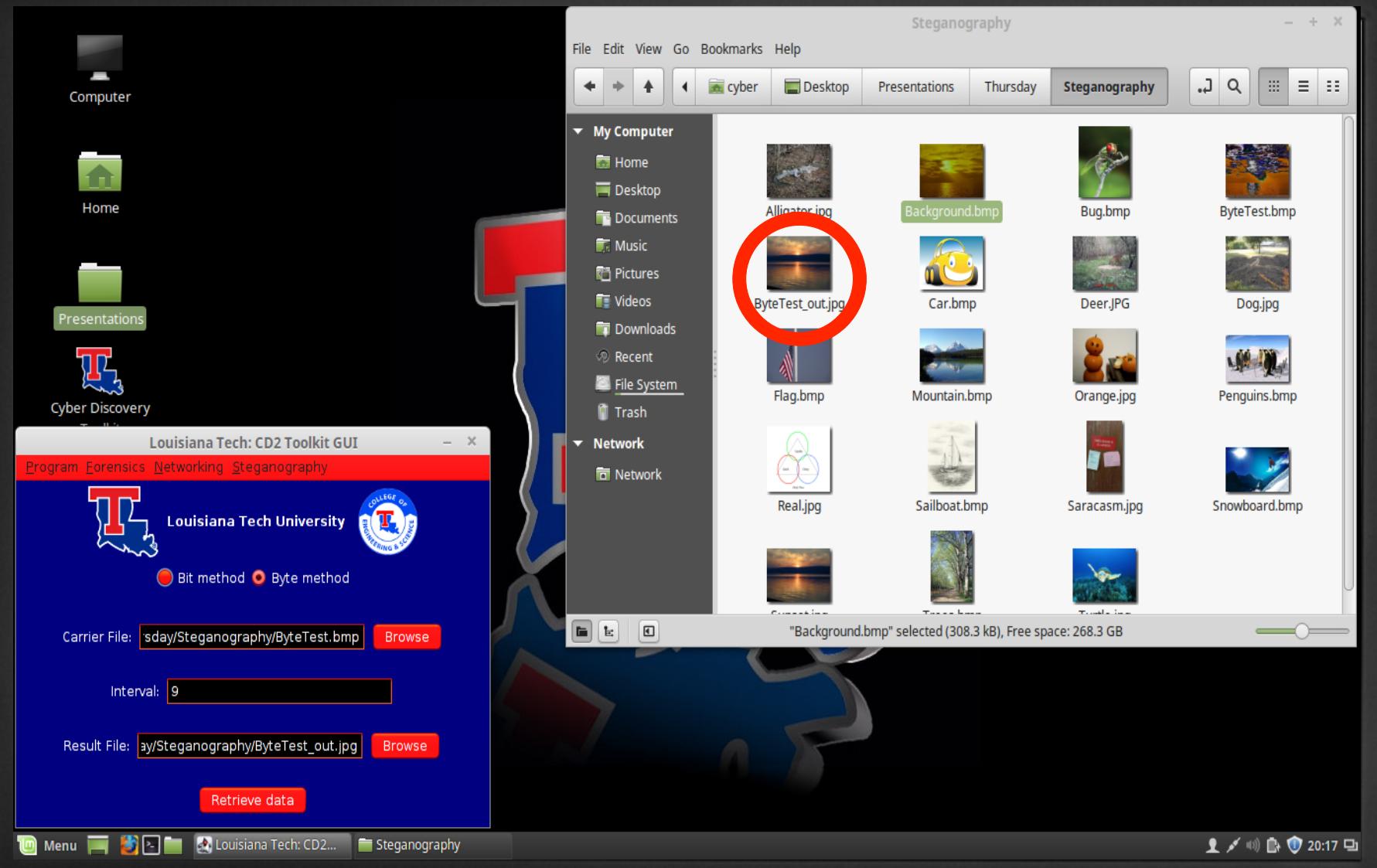


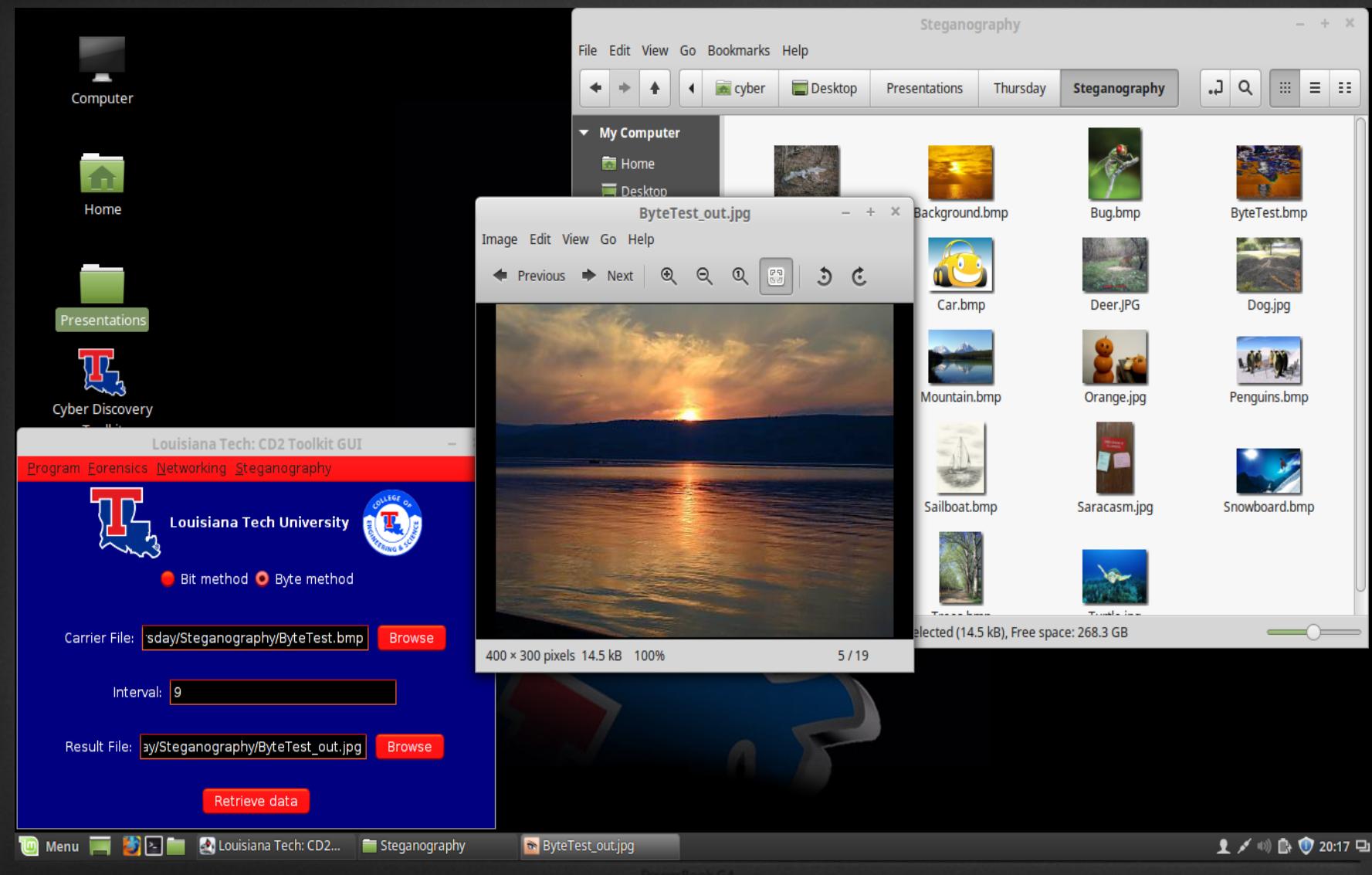


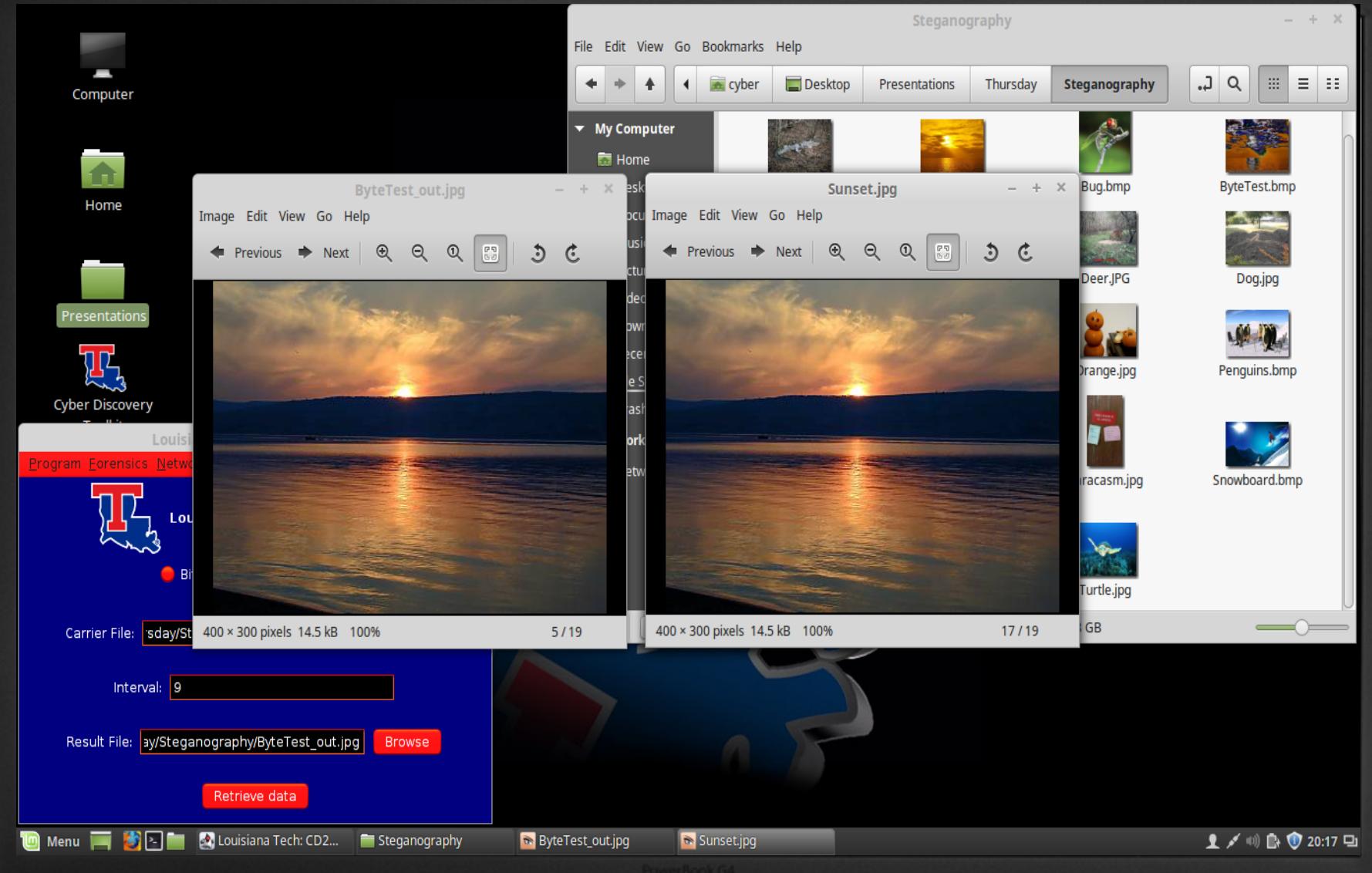
Menu Louisiana Tech: CD2... Steganography ByteTest.bmp Background.bmp

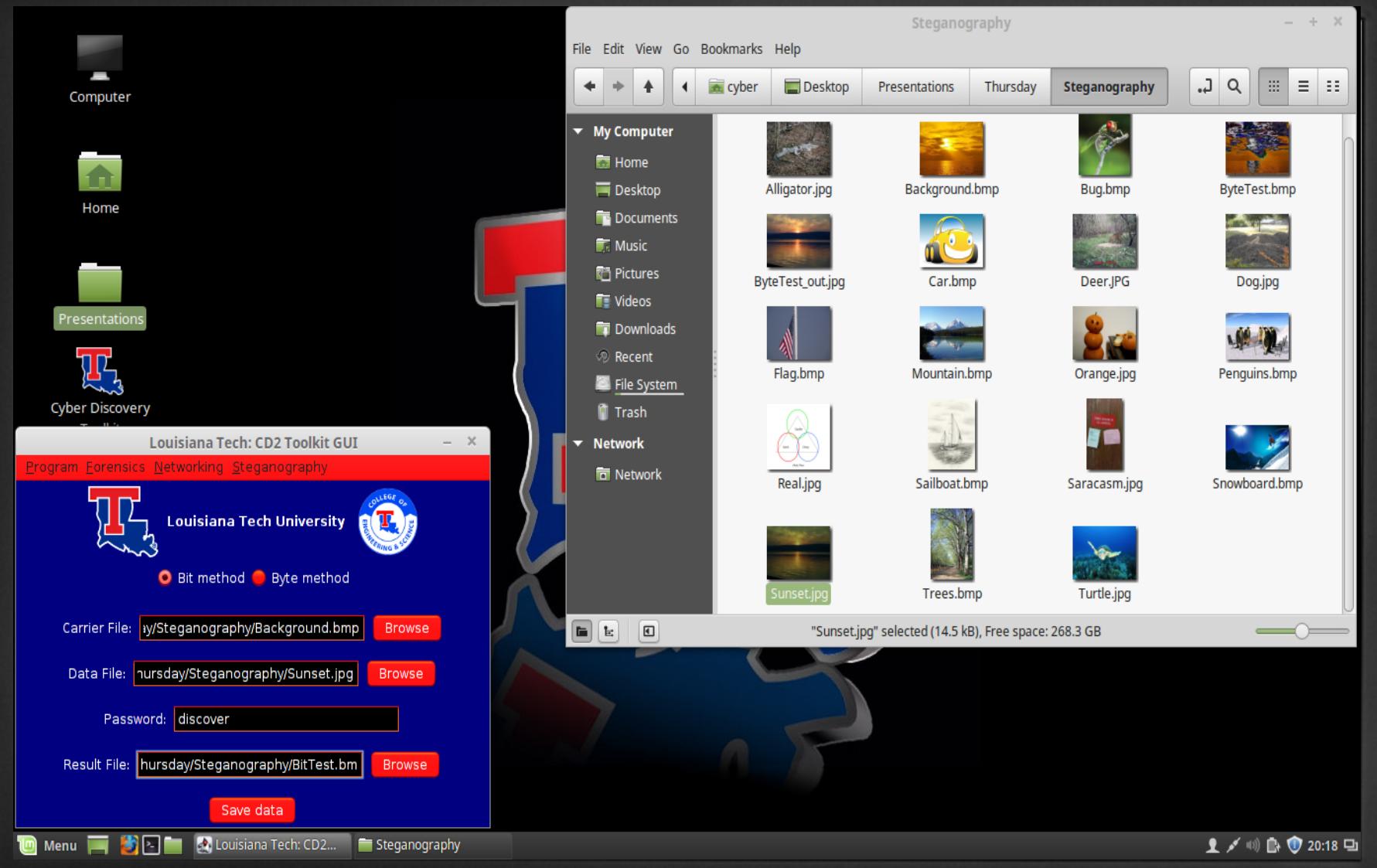
PowerBook G4



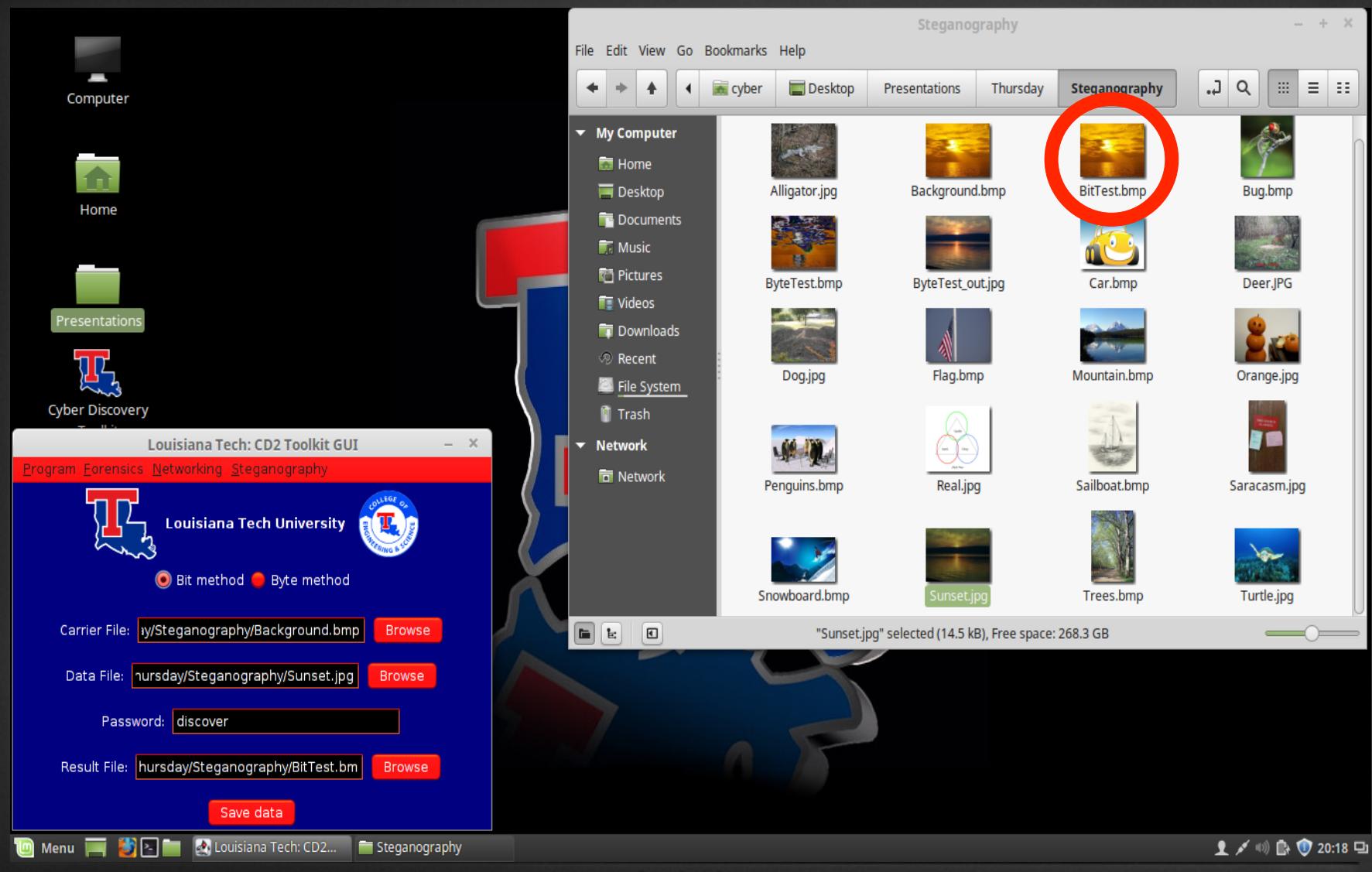




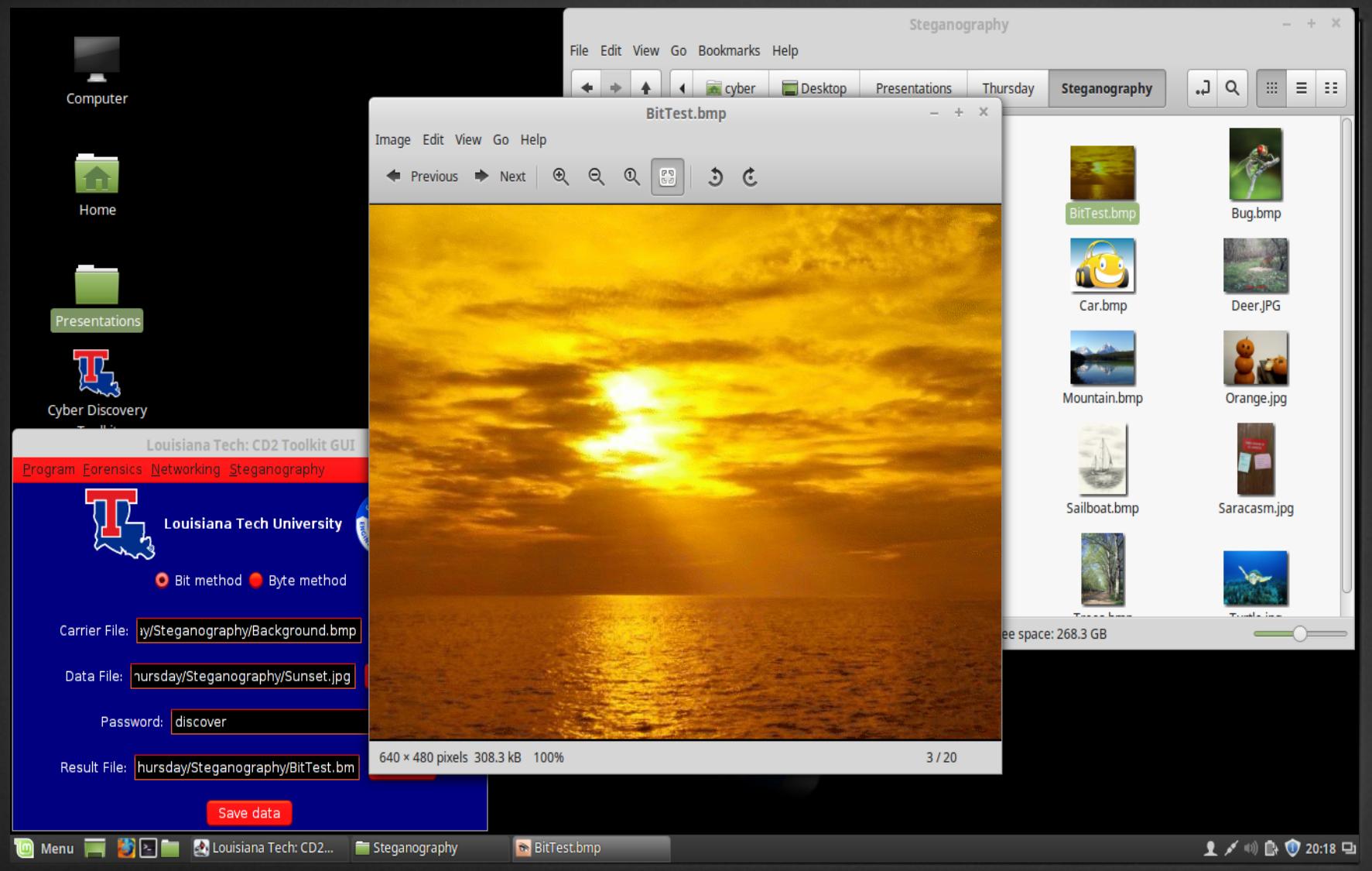




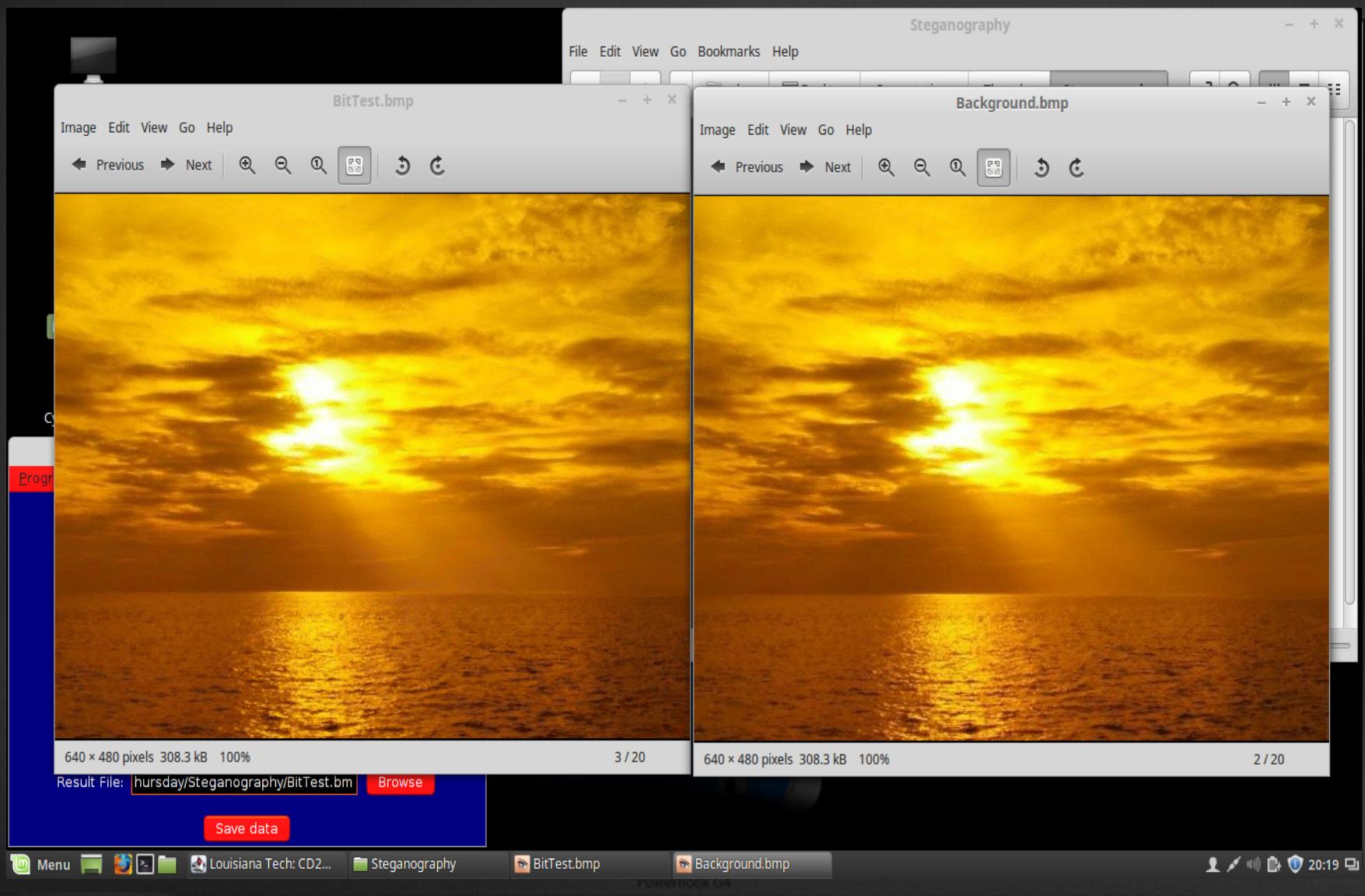
PowerBook G4



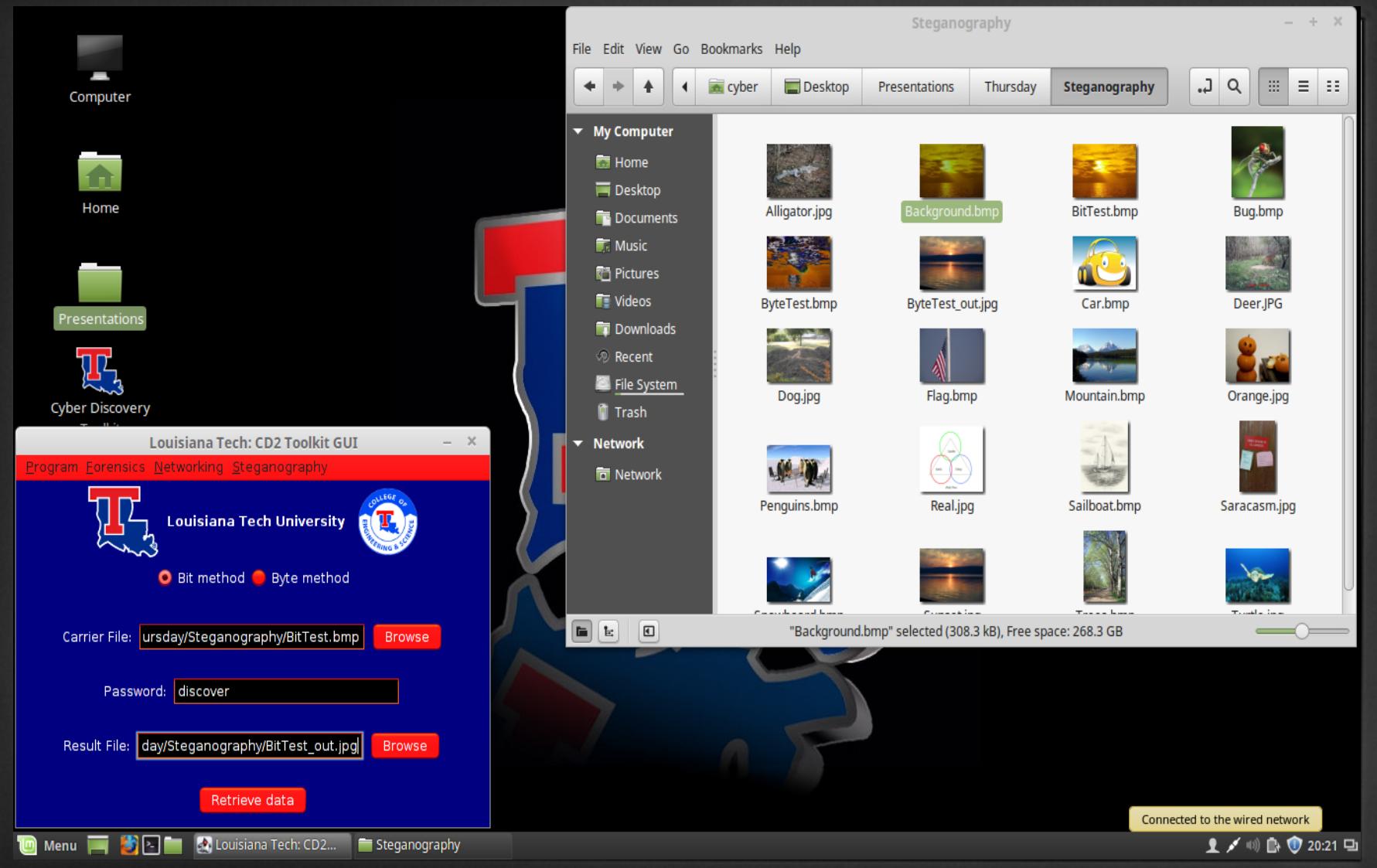
PowerBook G4



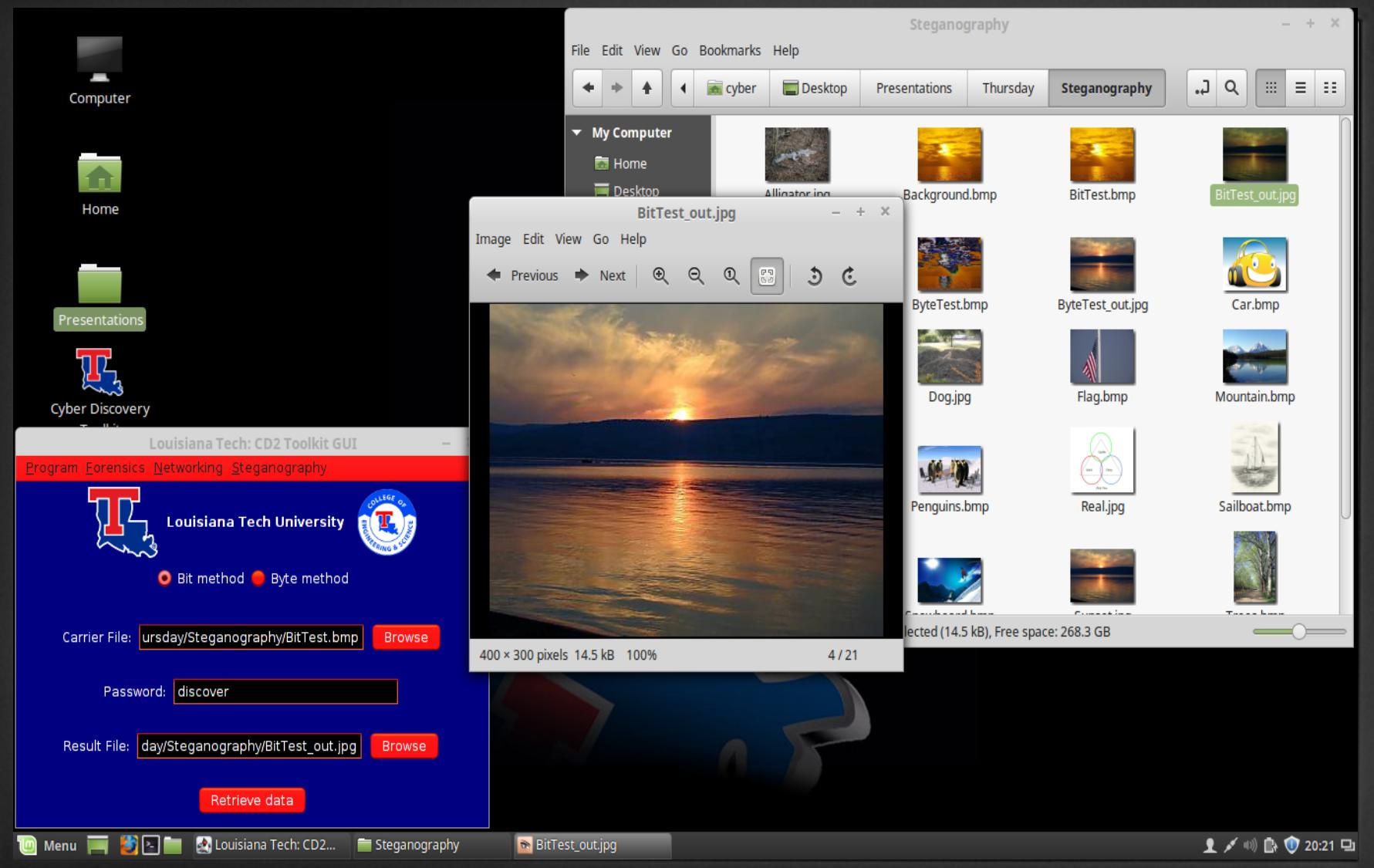
PowerBook G4

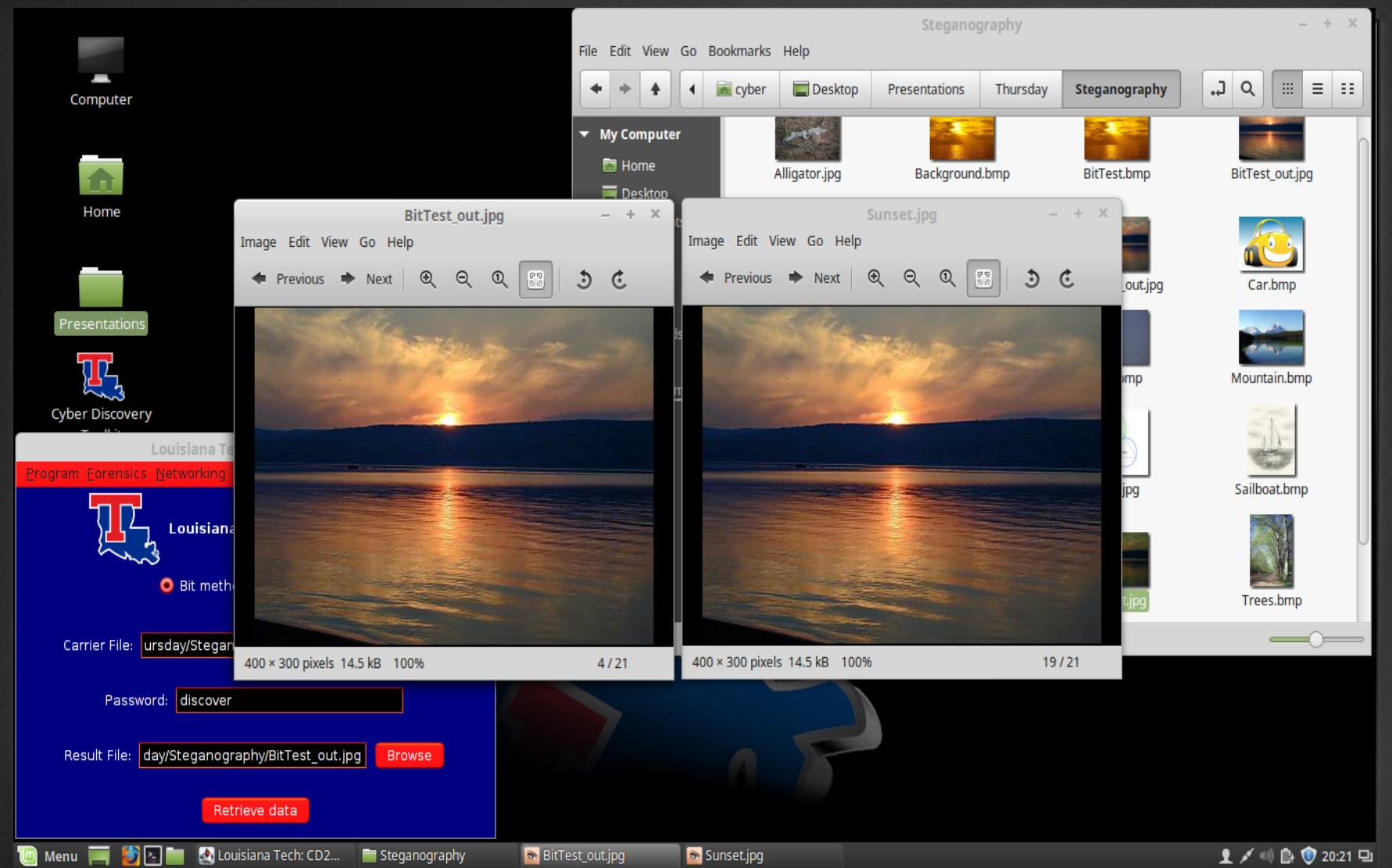


L Menu Louisiana Tech: CD2... Steganography BitTest.bmp Background.bmp 20:19









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 the Toolkit to insert and extract files

