Assignment 7:

Digital Steganography (Total 100 Points)

CYSE 301: Cybersecurity Technique and Operations

Carl Lochstampfor
MIDAS ID: cloch001
UIN: 01290201

April 8, 2026

Task-A: [10 points]

Explain what steganography is and how it differs from cryptography?

Steganography hides secret messages within ordinary files, such as images or audio. The word means "secret writing" in Greek. The carrier file looks normal, so no one suspects any hidden data.

Cryptography turns a message into unreadable text with encryption and a secret key. While the content is protected, it's obvious a secret message is being sent; people can see but not read it.

Thus, Cryptography hides a message's content; steganography hides its existence. Used together, one can encrypt a message and then hide it in a file, protecting both the message and its presence.

Task B : Lab Preparation:

- Access Windows7 VM in CCIA to open steghide command prompt (available in windows 7 Desktop)

You need to use **steghide**, not ~~tool~~ to complete this assignment.

You may refer to the lecture for Module-6 to learn about using steghide tool. **Please submit the screenshot as a proof for all the steps/commands**

1. **[10 Points]** Create a text file containing the answers to the following questions:
   - What are your name and current date and timestamp?
   - What is your expected grade in this course?

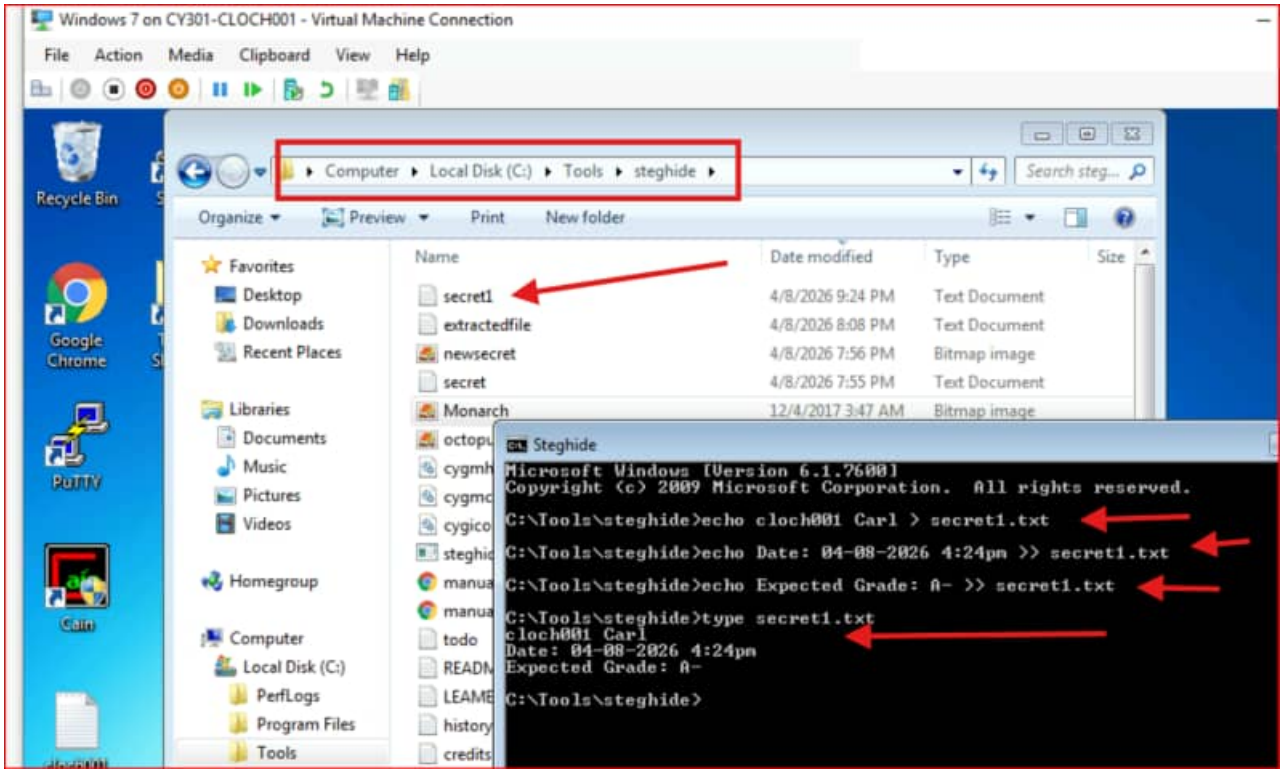
Commands >>

A. **echo cloch001 Carl > secret1.txt** (create the folder with my MIDAS ID & Name)

B. **echo Date: 0408-2026 4:24pm >> secret1.txt** (adds the current Date and Time to text file)

C. **echo Expected Grade: A- >> secret1.txt** (adds expected grade to the same text file)

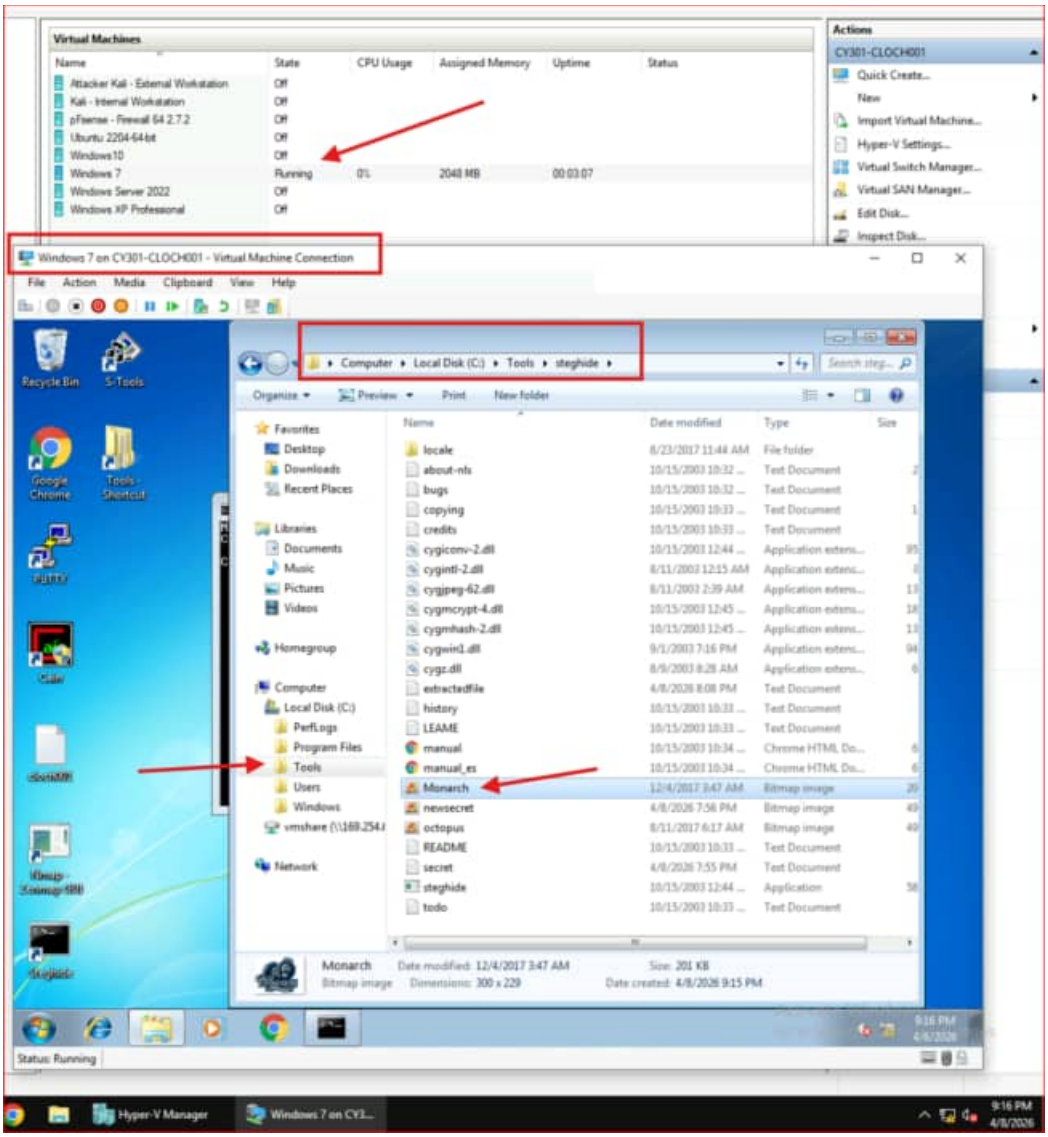
D. **type secret1.txt** (prints the contents of the text file to the terminal)



2. **[40 Points]** Complete the following tasks using steghide command:

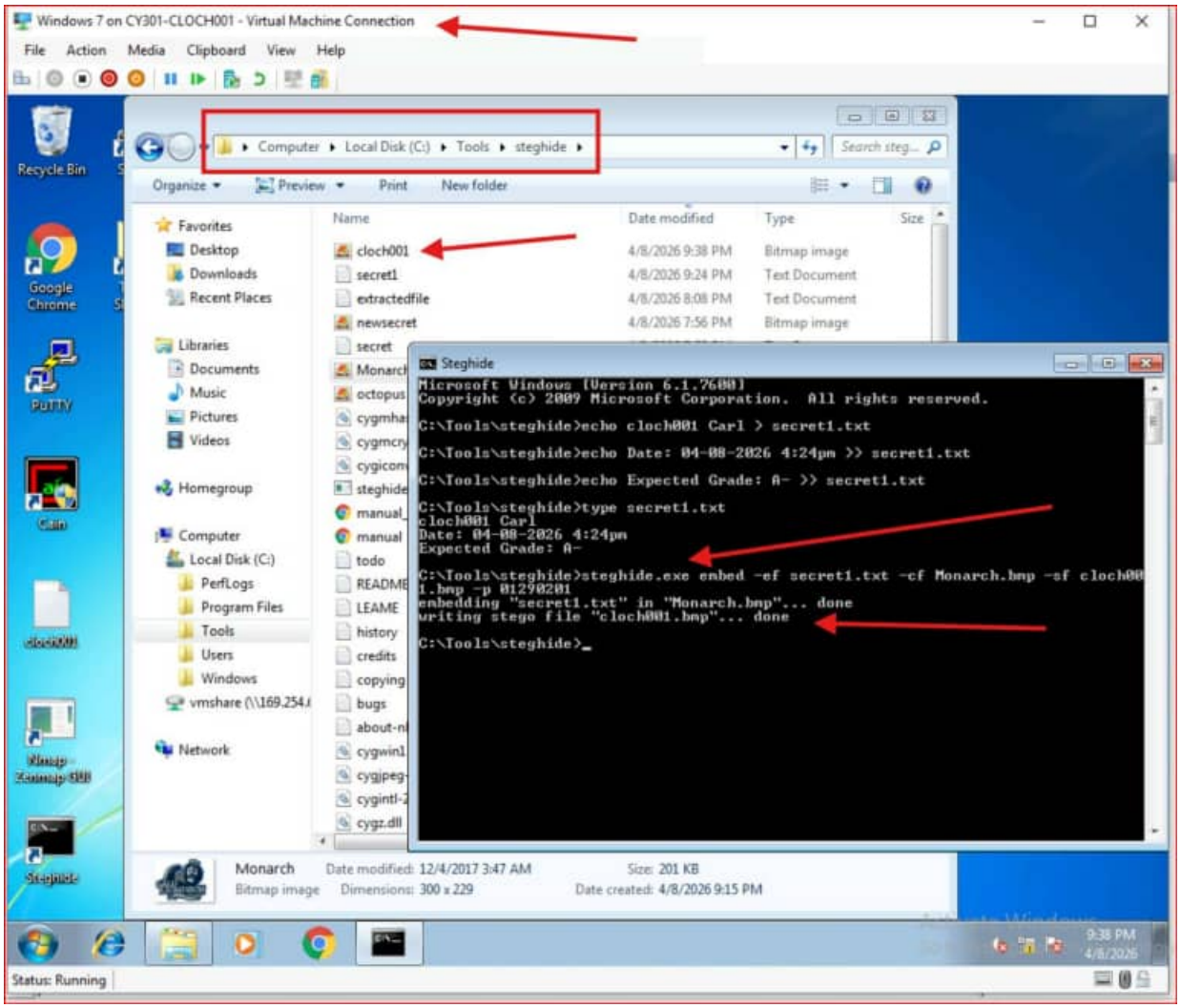
   a. Use **steghide** to *hide this text file* in the cover image, " Monarch.bmp.", which you can find in Windows7 under VMShare folder--> Lab-Resources--> Module

First, I copied first the Monarch.bmp image to the steghide folder for easier access.

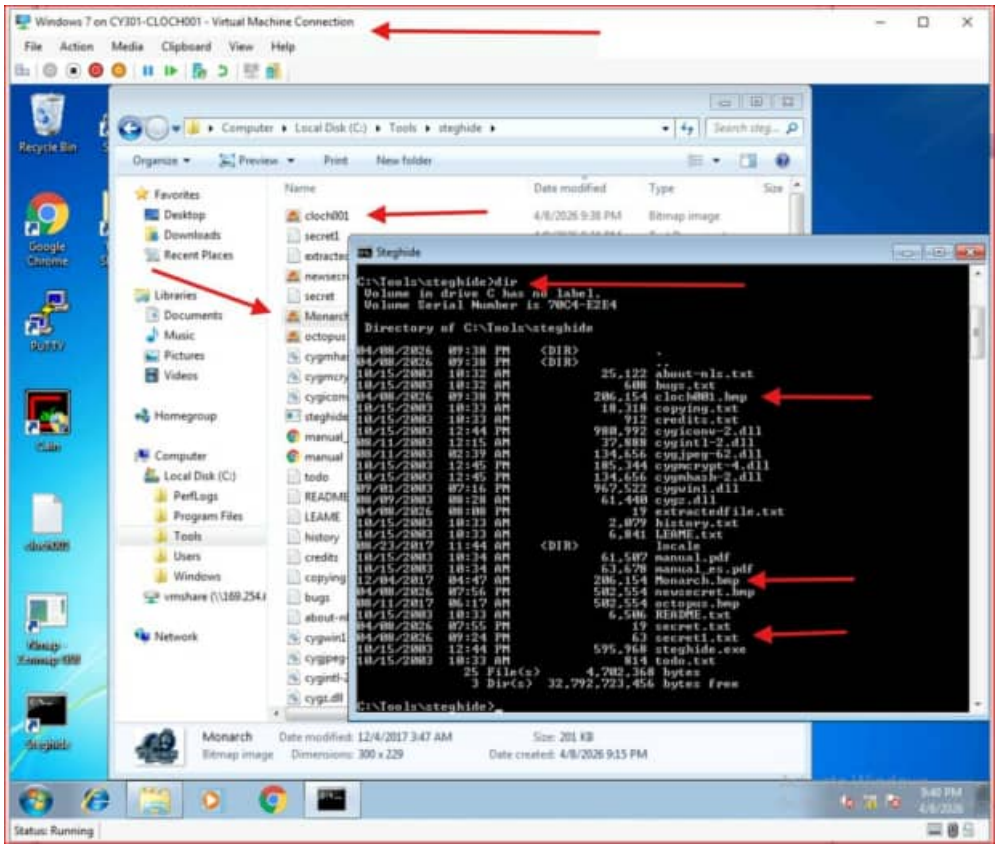


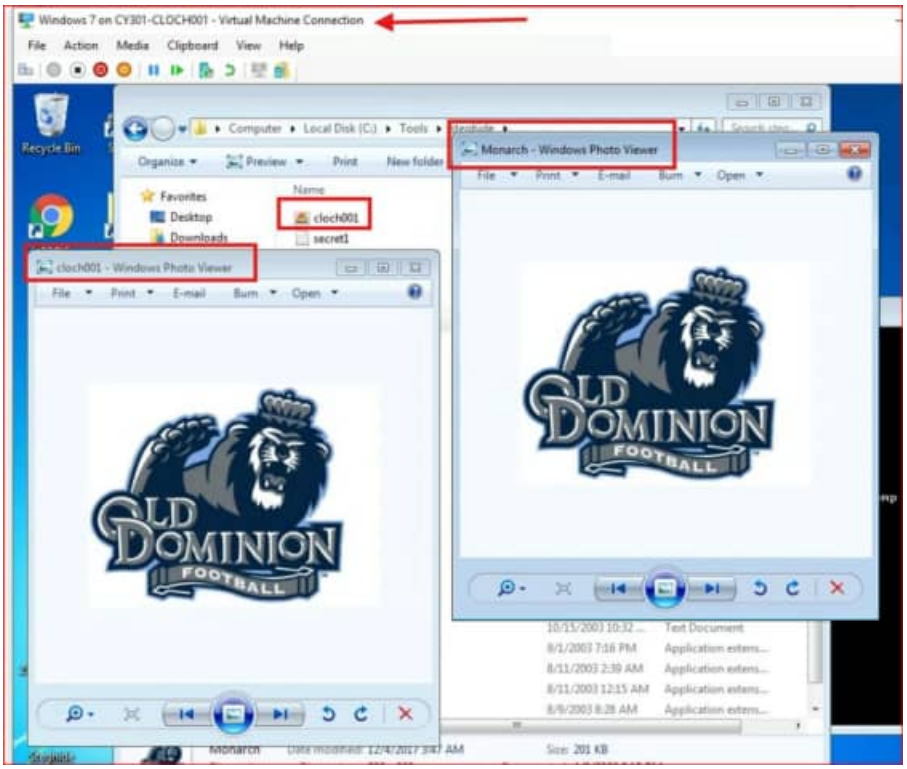
b. Use your **Midas ID** (all lowercase) as "YourName.bmp" for example "**svatsa.bmp**" as the name of the STEGOfile.
c. Use your own **UIN** (for example, 01000123) as the password.

- **Command >>** steghide.exe embed -ef secret1.txt -cf Monarch.bmp -sf cloch001.bmp -p 01290201
  - -ef secret.txt = the file to embed (your secret)
  - -cf Monarch.bmp = the cover image
  - -sf cloch001.bmp = output stego file name (my MIDAS ID is cloch001)
  - -p 01290201 (my UIN is the password to the file)



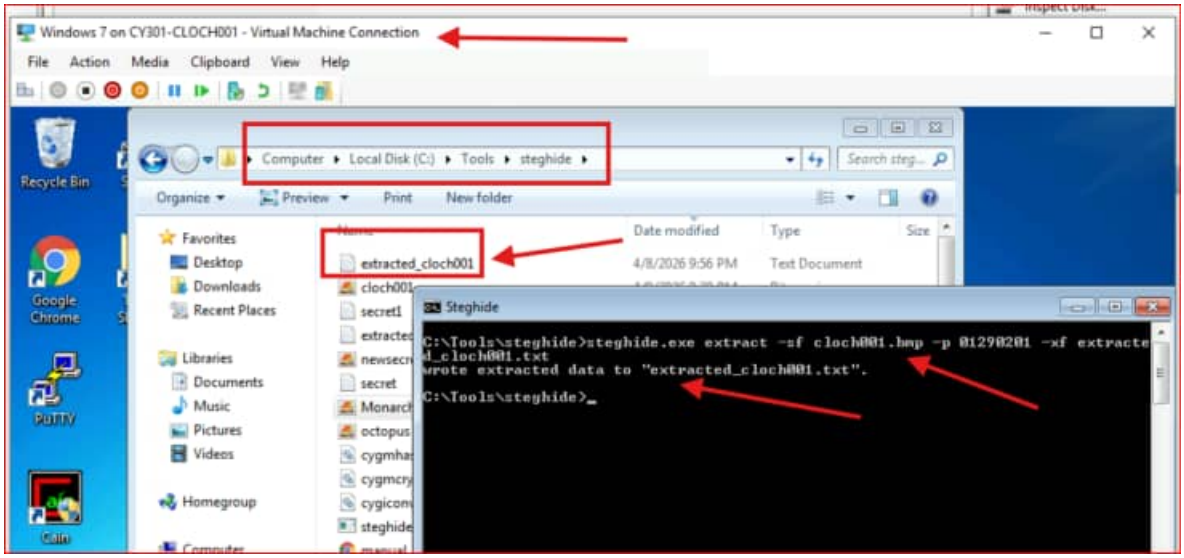
d. List the contents of the current directory/folder to verify if the stego file is created or not.
   - **Command >>** dir





3. **[20 Points]** Extract the secret message by executing steghide command and save in a file named "extracted_YourName.txt".

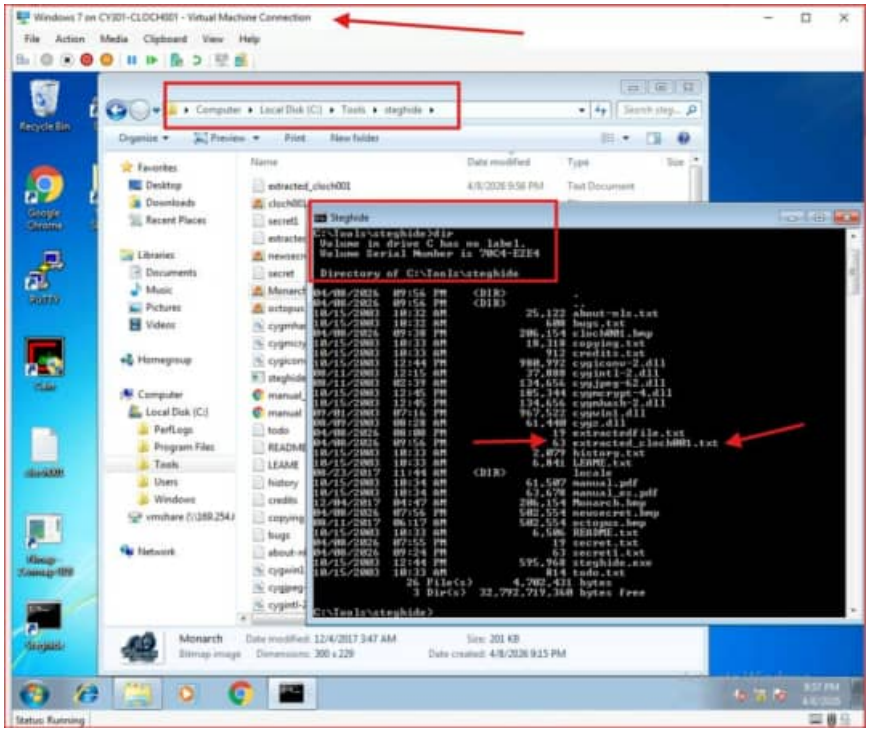
   - **Command >>** steghide.exe extract -sf cloch001.bmp -p 01290201 -xf extracted_cloch001.txt



4. **[10 Points]** Execute the command to list the contents of the current directory in CMD to verify whether the extracted textfile with secret message has been extracted or not.

   You should see textfile there because it was hidden in the image file and appeared after extracting the image file in the previous step.

   - **Command >>** dir



5. **[10 Points]** Execute the command to display the contents of the extracted file you revealed.

   - **Command >>** type extracted_cloch001.txt