**Steganography Assignment**

**Exercise 1**

**Incident Response Steps**

***Task #1***

List all the steps in a numbered list, and then separately explain each step in your own words.

When it comes to handling cybersecurity incidents, it is important to be **prepared**. The first step is all about getting ready ahead of time. This means setting up clear policies, procedures, and tools. It also involves making sure everyone knows their role and responsibilities. Regular training and drills help keep everyone sharp and ready to respond effectively.

Next up is **detection**. It is like having a keen eye watching over everything. We keep a close watch on our systems and network traffic, looking for any signs of trouble. We use tools like intrusion detection systems and carefully analyze logs to catch anything suspicious before it becomes a bigger problem.

Once we spot something fishy, it is time for **analysis**. This is where we roll up our sleeves and dive deep into the incident. We gather all the data we can get our hands on and piece together what happened. Understanding the scope and impact of the threat helps us figure out the best way to respond.

**Containment** is like putting up a strong barrier to keep the bad stuff from spreading. We take quick action to limit the damage and isolate any affected systems. By acting fast, we can stop the incident from getting worse and protect the rest of our organization.

**Eradication** is all about getting rid of the threat for good. We hunt down any malicious files, patch up vulnerabilities, and close off any backdoors that attackers might have left behind. It is like cleaning house to make sure our environment is safe and secure once again.

**Recovery** is the process of getting back on our feet after an incident. We work to restore affected systems and services to normal operation. This might involve restoring data from backups, reinstalling software, and making sure everything is clean and free from any lingering threats.

Finally, there is the **lessons learned** step. We take a step back and reflect on what happened. We look for ways to improve our response process for next time. Maybe there are new tools we need to add to our arsenal, or perhaps we need to tweak our procedures. It is all about learning and growing from our experiences.

**Incident Response Phases**

***Task #2***

List all the phases in a numbered list, and then separately explain phase step in your own words.

1. **Preparation:** Before any trouble starts, it is important to have everything set up. This means creating rules, plans, and teams to handle problems, and making sure everyone knows what to do through practice.
2. **Detection:** Detection means catching security issues as soon as possible. We keep an eye on our systems and the way data moves around to notice if anything fishy is happening. Special tools help us find any unusual activity that might mean trouble.
3. **Analysis:** Analysis is about figuring out the who, what, and how of a security problem once we have spotted it. We gather and study all the info we can get, like logs and data traffic, to see what went wrong and what got affected.
4. **Containment:** Containment is about putting a lid on the problem to stop it from getting worse. We take steps to keep the trouble isolated and prevent it from messing with other parts of our systems, like shutting down accounts or blocking bad guys' access.
5. **Eradication:** Eradication is like giving our systems a deep clean after a security scare. We hunt down and get rid of any nasty stuff that might have snuck in, like viruses or sneaky backdoors, so everything is safe again.
6. **Recovery:** Recovery is about getting things back to normal after a security hiccup. We restore any lost data, reinstall software if needed, and make sure everything is free from bad stuff before we go back online.
7. **Lessons Learned:** In the end, we take a good look at what happened and learn from it. We figure out what we did well and what we can do better next time, so we are even more prepared to handle any future problems.

**Top of Form**

**Incident Response Policy**

***Task #3***

Explain what the purpose of an incident policy is in your own words.

An incident response policy is like the foundation of a building for an organization's cybersecurity. It is super important because it gives clear instructions on how to deal with security problems. Without it, the organization would be lost when facing breaches or threats. The policy helps in many ways, like explaining what to do when there is a problem, who is responsible for what, and how to fix things. It also makes sure the organization follows all the rules and talks to the right people when something goes wrong. Keeping the policy up-to-date and making sure everyone knows what to do helps the organization stay safe from cyber threats, protecting its stuff, operations, and reputation.

**Top of Form**

**Incident Response Plan**

***Task #4/#5***

Explain what an IRP is, and what purpose does it play in your own words.

An incident response plan (IRP) is like a playbook that helps organizations deal with cyber-attacks in the best way possible. It is important because it gives a step-by-step guide on how to handle different types of security problems. The plan covers everything from understanding what is happening in the organization to forming a team with specific jobs, figuring out how to spot and fix problems, and communicating with everyone involved. It also includes training for the team and making sure everything stays up-to-date. The plan's main goal is to make sure the organization can respond quickly and effectively to cyber-attacks, following all the rules and keeping good records along the way.

**Recon**

***Task #6***

Explain what an enumeration is, and what purpose does it play in your own words.

Enumeration in cybersecurity means gathering information about a network, computer, or program in an organized way. It involves finding out what resources, services, and weaknesses are present. The main aim is to understand how the system is set up and where it might be vulnerable to attack. Attackers use enumeration to find ways to get into a system without permission and to gain more control once they are inside. On the other hand, security professionals use enumeration to check for weaknesses in a system and to make it stronger against potential attacks. It helps them find and fix problems before attackers can exploit them, making the organization's overall security better.

**Exfiltration**

***Task #7***

Explain what an tunneling is, and what purpose does it play in your own words.

Tunneling is like sending a secret message inside another message so it can go through places where the original message could not go. It makes a safe path or "tunnel" through networks that might not be safe or compatible. The main goal is to make sure information can travel safely over networks that might not be safe, like the internet. It helps keep data private, intact, and available. Tunneling is used a lot in Virtual Private Networks (VPNs) to make secure connections between faraway users and company networks, letting them access resources even if there are restrictions or censorship on the internet. Also, tunneling protocols like Secure Shell (SSH) and Secure Socket Tunneling Protocol (SSTP) are used to safely access faraway systems or services over public networks, making sure data stays private and safe while traveling through different kinds of networks.

**Communication**

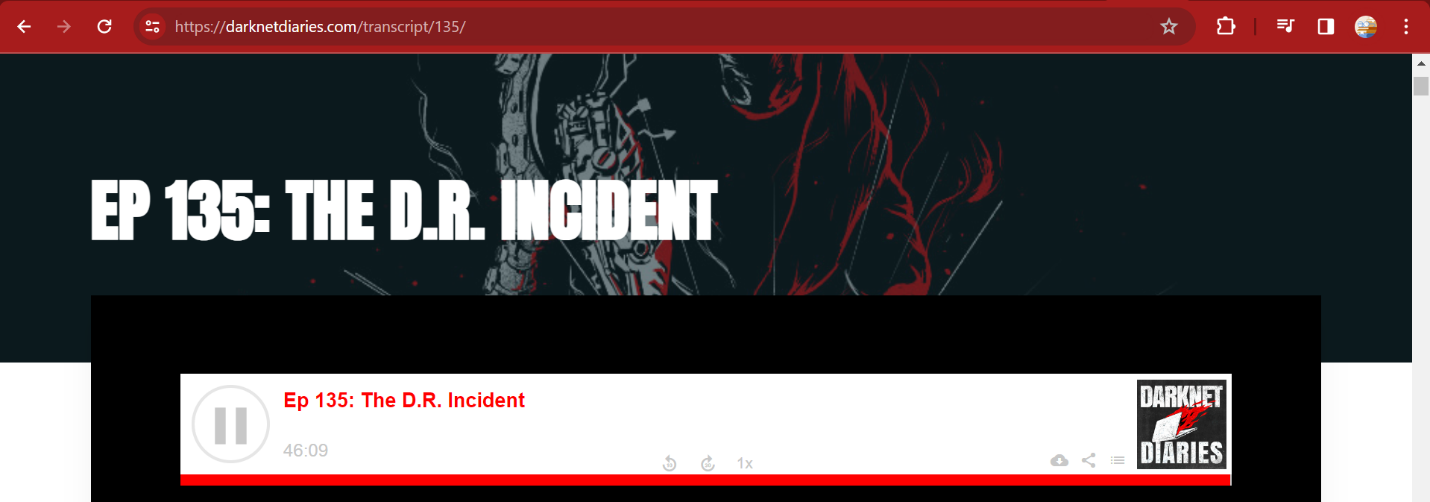
***Task #8***

Explain what a pem file is, and what purpose does it play in your own words.

A PEM (Privacy Enhanced Mail) file is like a digital container that holds secret codes used to keep online information safe. These codes can include things like certificates (which prove a website is secure), private keys (used to unlock encrypted messages), and public keys (used to send secure messages). These files are made in a way that computers understand and can use to keep internet connections safe. They are important because they help websites stay secure when you visit them, make sure only the right people can see sensitive information, and make sure software you download is safe to use.

**Incident Response – The Dominican Republic Incident**

1. Listen to this podcast on Incident Response:



The podcast delves into a cyber-attack targeting the Dominican Republic, detailing the intricacies of identifying the perpetrators, potential geopolitical implications, and the nation's response. It emphasizes the complexity of attributing cyber-attacks and navigating the interconnected landscape of international relations and cybersecurity. The episode showcases the importance of collaborative cybersecurity efforts, including information sharing and coordinated response strategies, to defend against sophisticated threats. Additionally, it underscores the significance of safeguarding critical infrastructure, particularly operational technology systems, against cyber intrusions. The episode prompts reflection on the evolving cybersecurity landscape and the ongoing challenges of securing digital systems amidst increasing global interconnectedness.

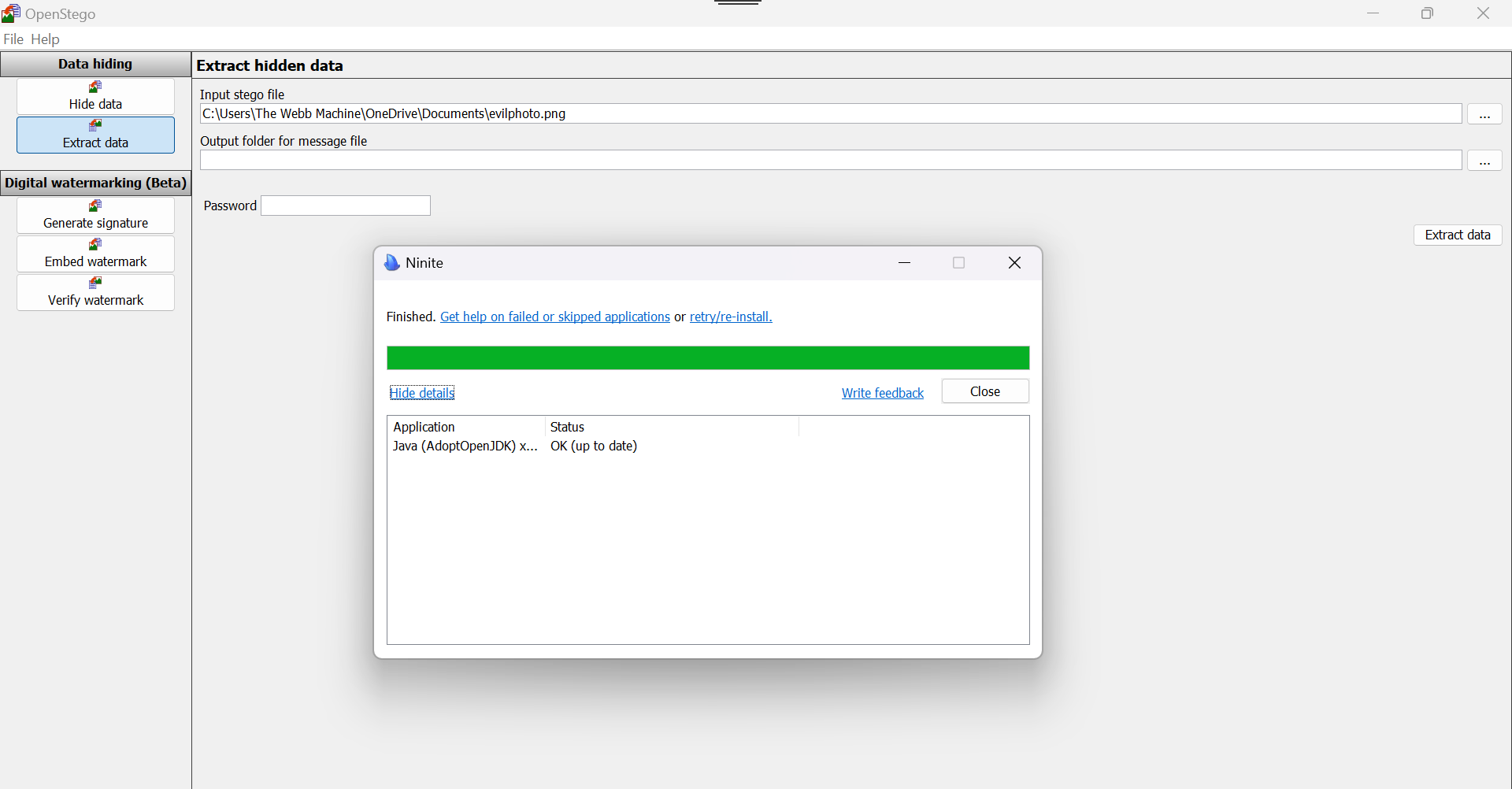
**Steganography – WINDOWS**

**Steganography Reveal Assignment**

**Note: maxresdefault-2003057562.jpg not available from:** [**https://github.com/ajay63/BlackTowerAcademy/blob/main/**](https://github.com/ajay63/BlackTowerAcademy/blob/main/)**, utilized evilphoto.jpg for this exercise**

*Task #1 Download:*

OpenStego from: <https://www.openstego.com/>



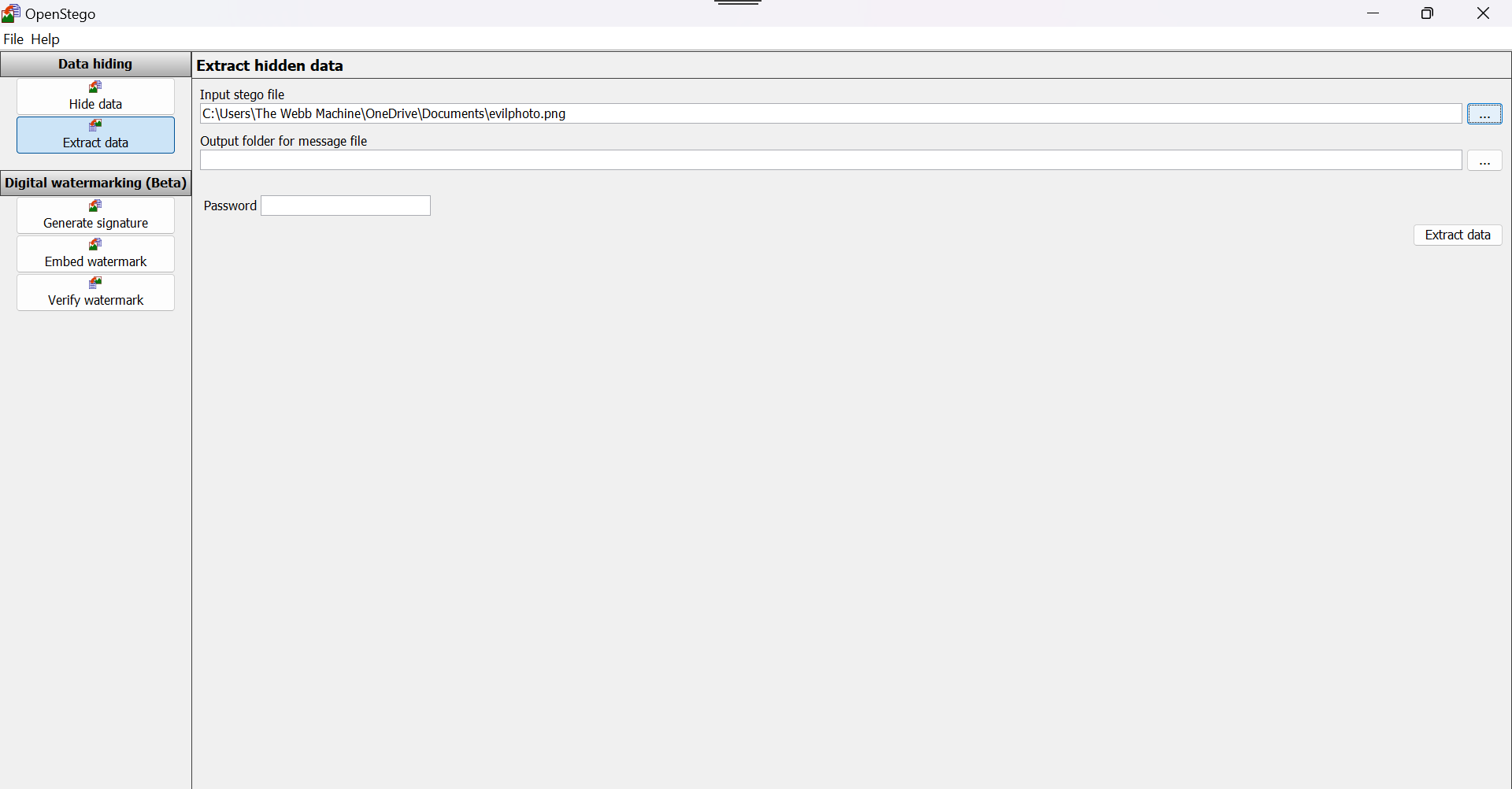
***Task #2-Dependencies:***

***It is likely if OpenStego fails to run, it is because it requires JAVA and you do not have it installed.***

***One can easily and quietly install Java from*** [***https://ninite.com/***](https://ninite.com/)

**Note:** OpenStego did not fail to run when downloaded on to my machine but I did install Java x64 bit just in case anyway.

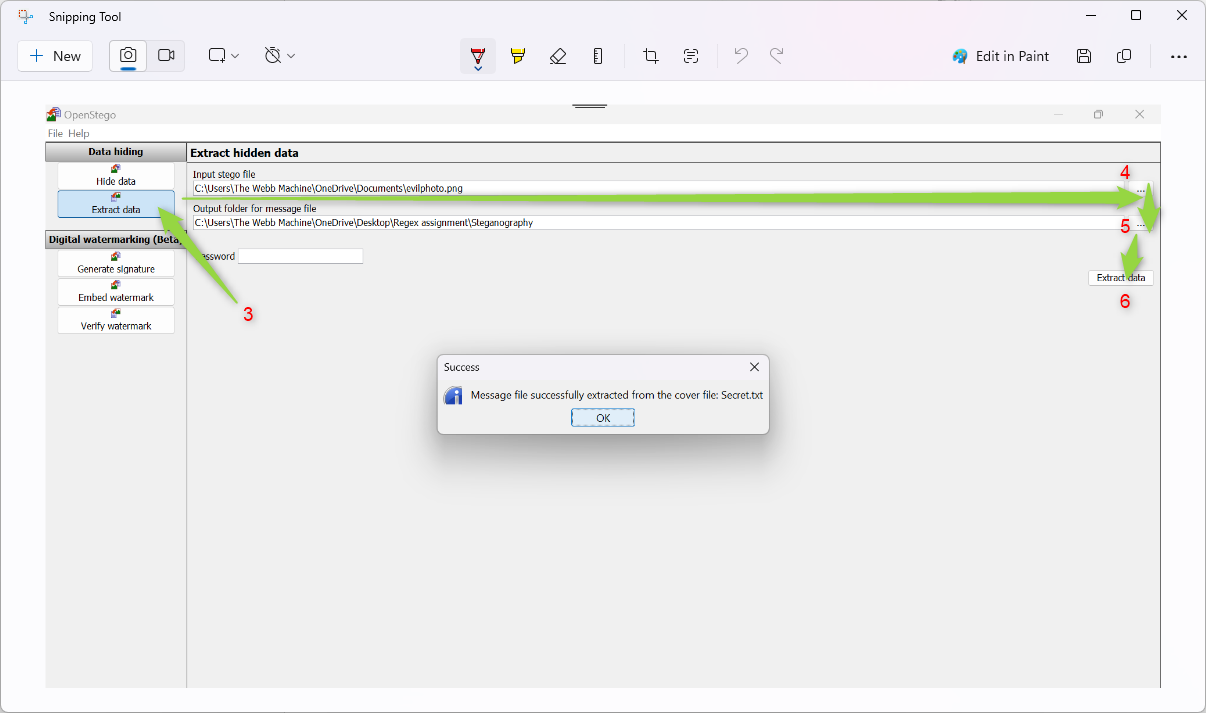
1. Download the Source File from GitHub: <https://github.com/ajay63/BlackTowerAcademy/blob/main/evilphoto.png>



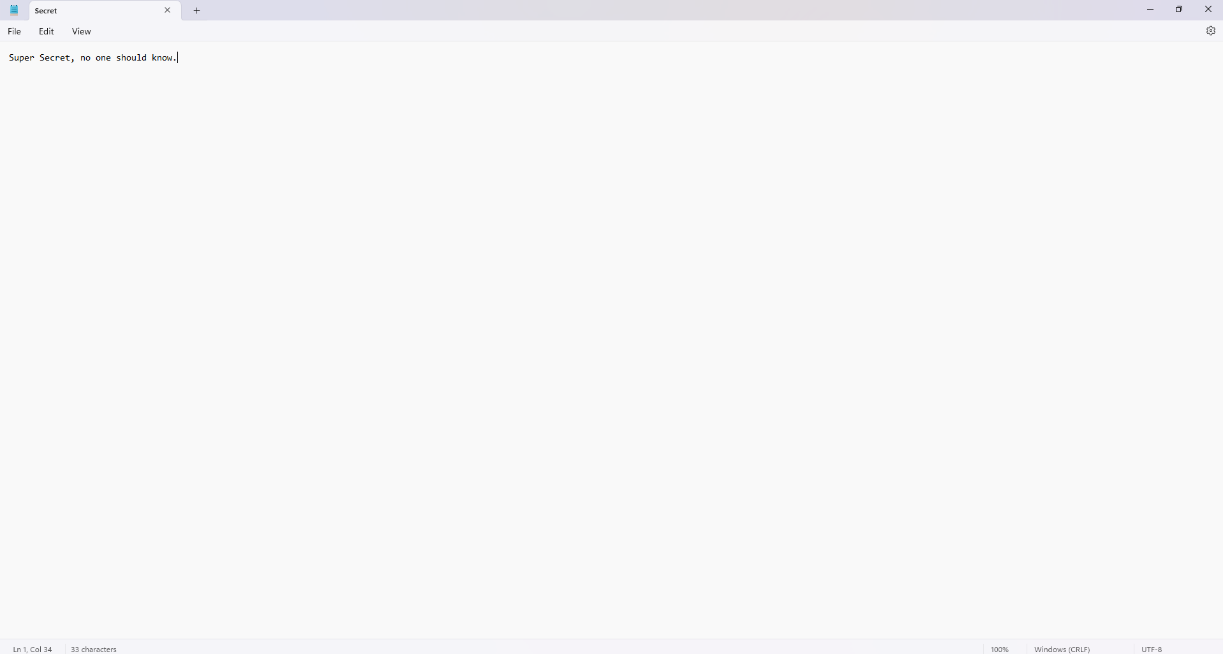
1. The evilphoto.png file was successfully downloaded from <https://github.com/ajay63/BlackTowerAcademy/blob/main/evilphoto.png> and is not loaded into Openstego for extraction.

***Task #3-Data Extraction***

1. Extract Data, 4. Button, select file downloaded, 5. Select folder for extraction, 6. Click on Extract Data



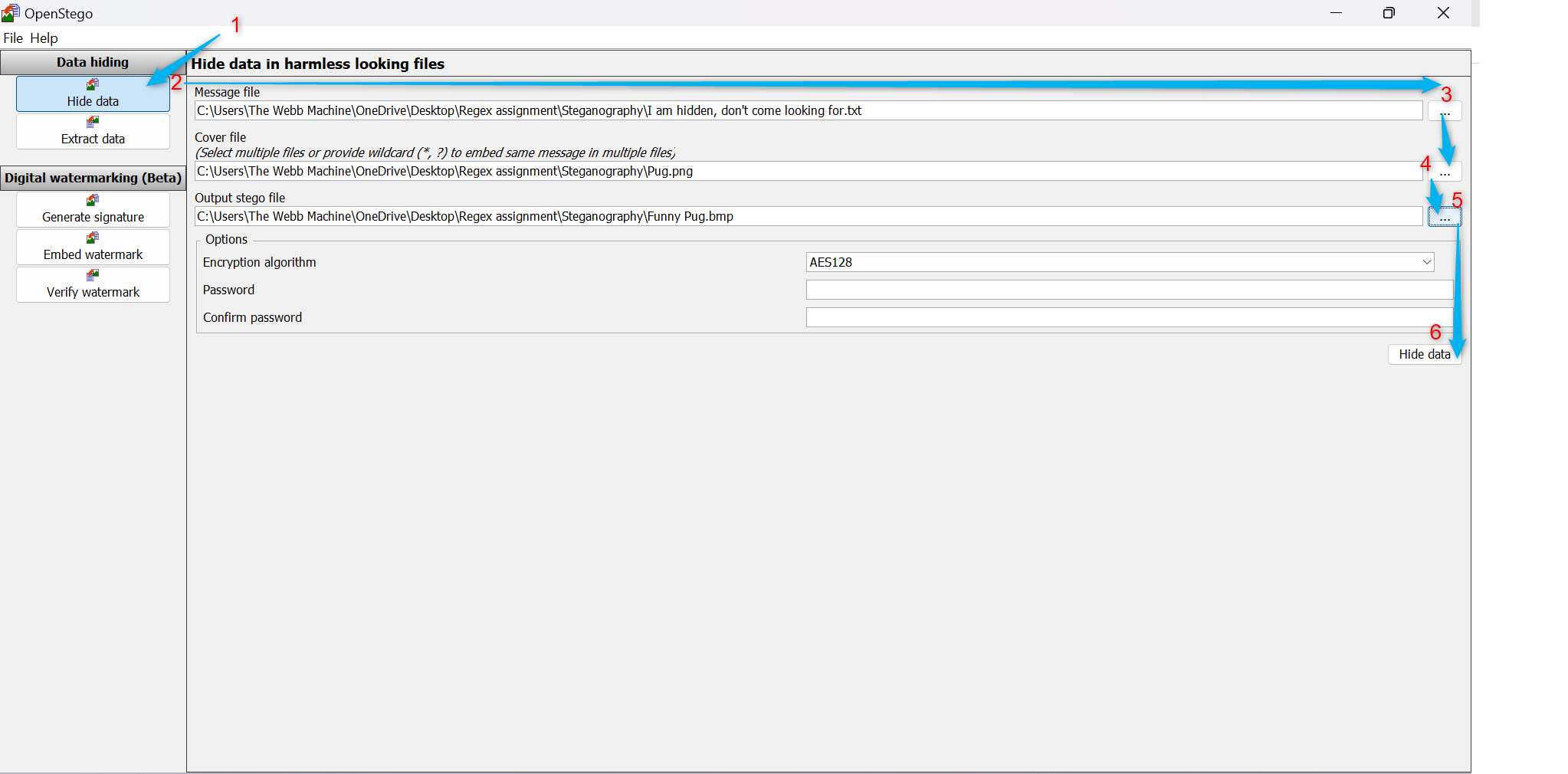
In the output folder it will generate a file. Open the file and read the secret message hidden in the picture.



**Steganography Hide Assignment:**

1. Select – Hide Data 2. Create a text file with a hidden message. (Save the file)

3. Select the text file with the hidden message. (Message File) 4. Select a funny picture you already have. (Cover File)

* 1. 5. Select a location and file name for your stenographic file. (Output File) Save it as a .png file
  2. 6. Click Hide Data
  3. 

Classmate Data Extraction Assignment: Embed a secret in an image, then share the file with a classmate, and have him read the secret message back to you.

Sent Classmate stego image below with hidden message:



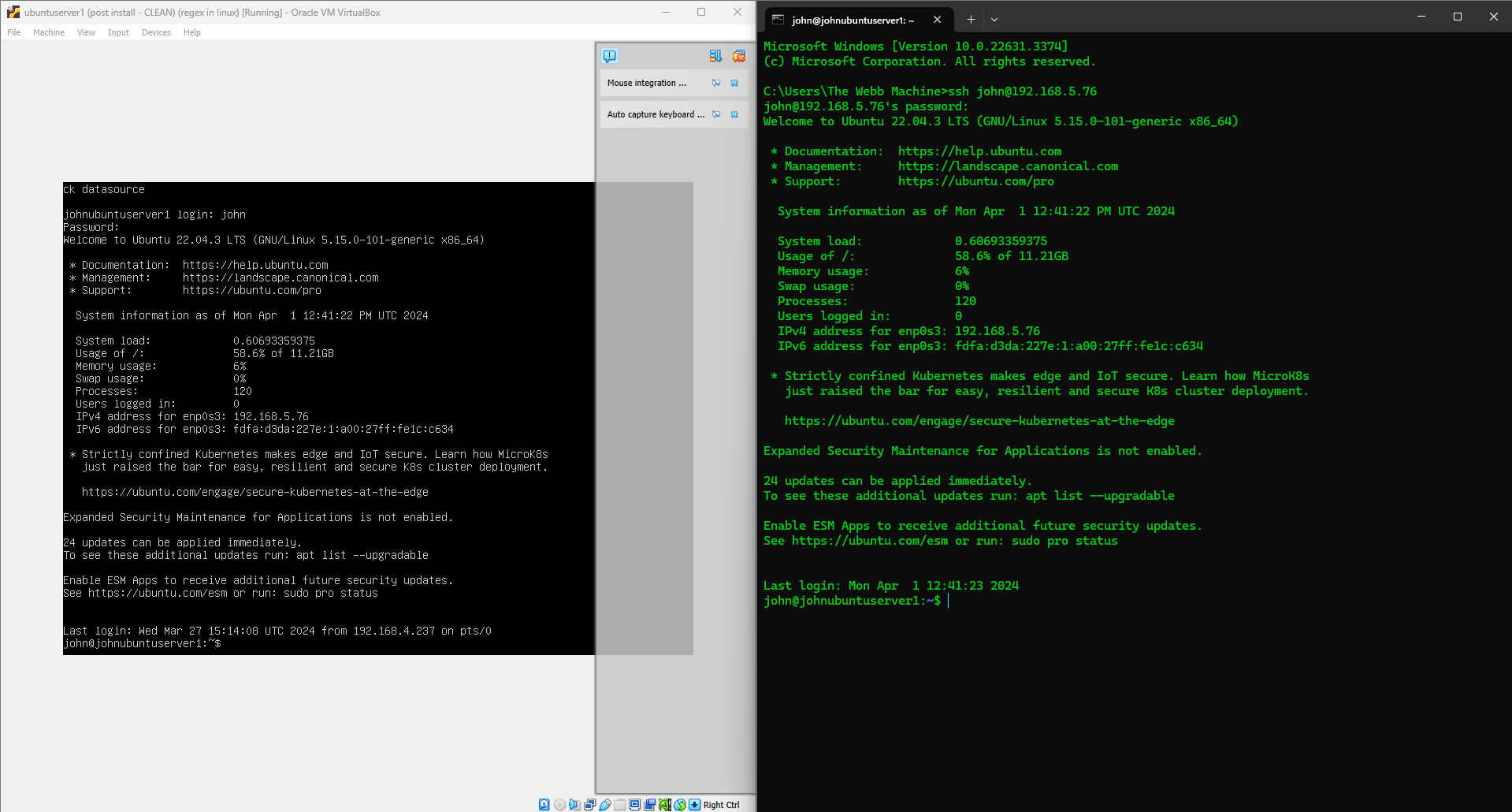
Classmate sent me the stego image below:

Extracted the image using Open Stego:

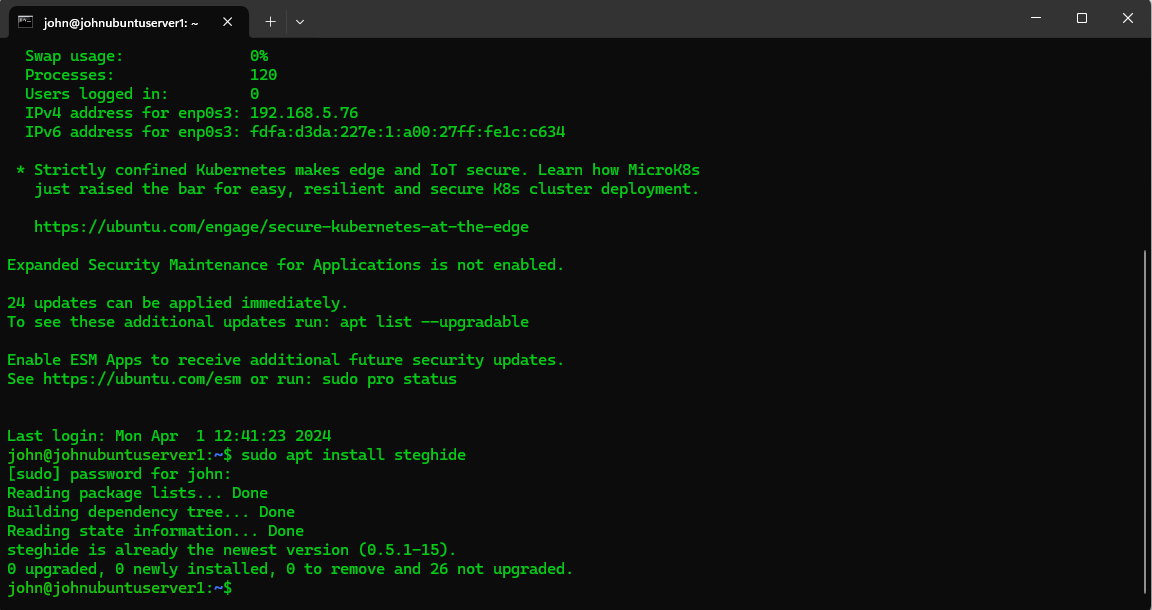
Found the hidden message:

Steg hide Assignment:

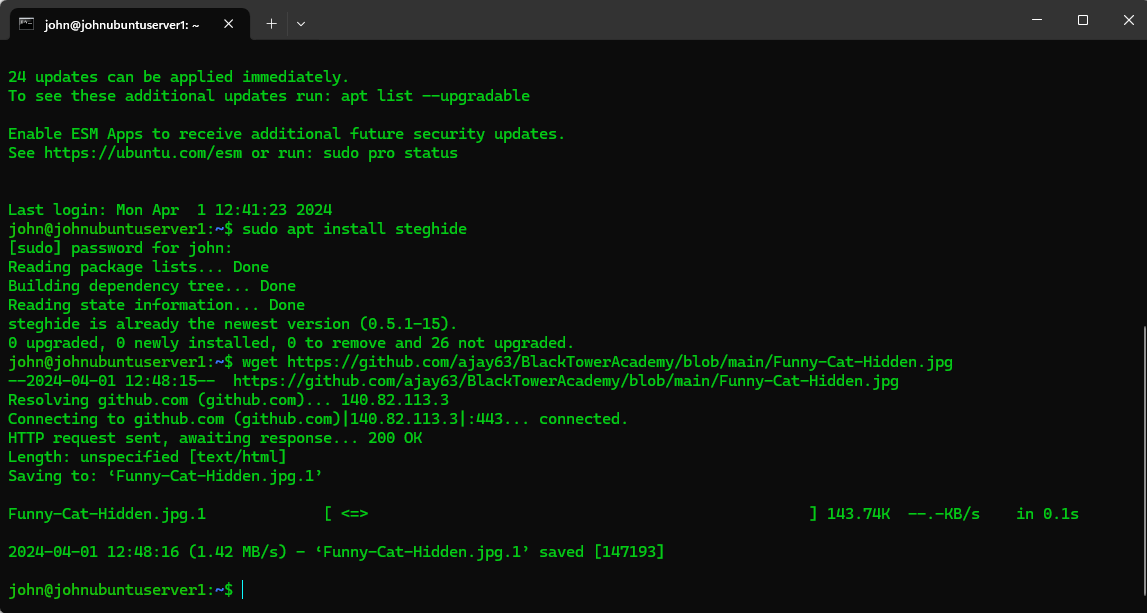
Open and Run Virtual Box Ubuntu Linux VM and ssh into Ubuntu Linux server in the host CLI:



1. Install Steghide: Installed Steghide using the following command sudo apt install Steghide



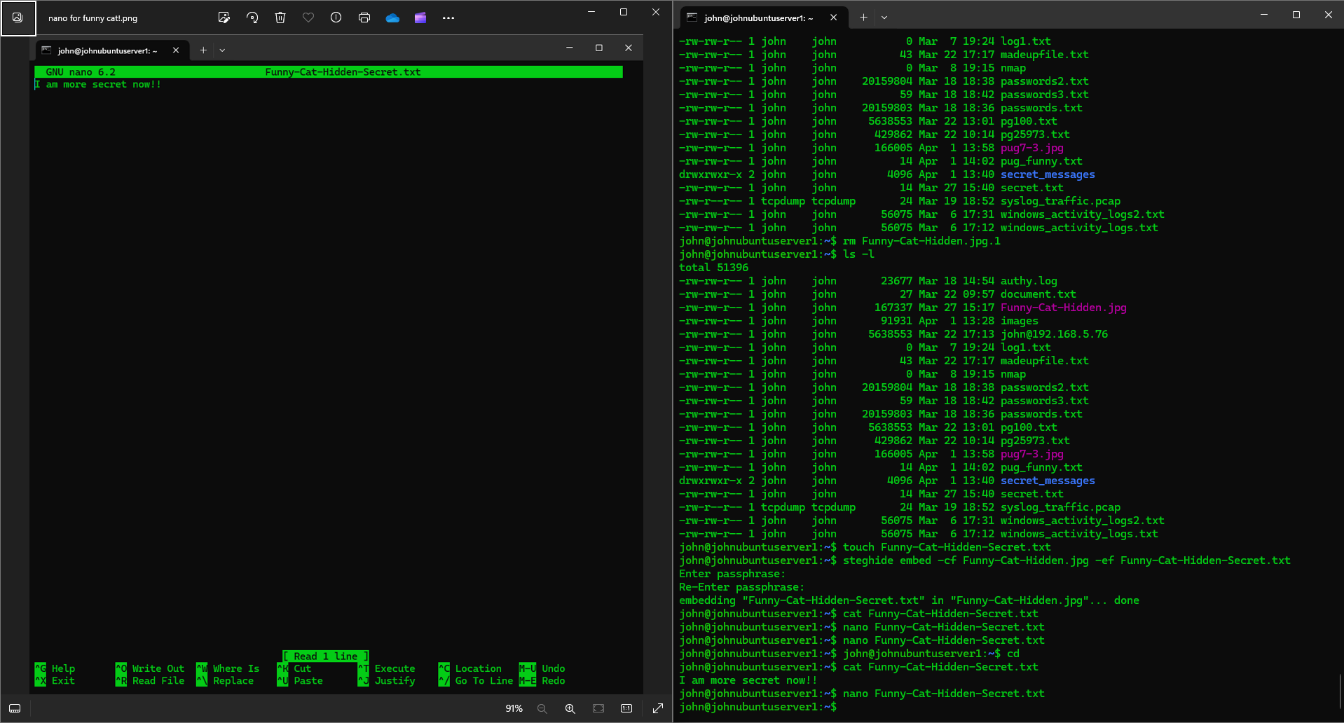
1. Download and extract the secret message from <https://github.com/ajay63/BlackTowerAcademy/blob/main/Funny-Cat-Hidden.jpg>, extracted jpg file using the following command wget https://github.com/ajay63/BlackTowerAcademy/blob/main/Funny-Cat-Hidden.jpg



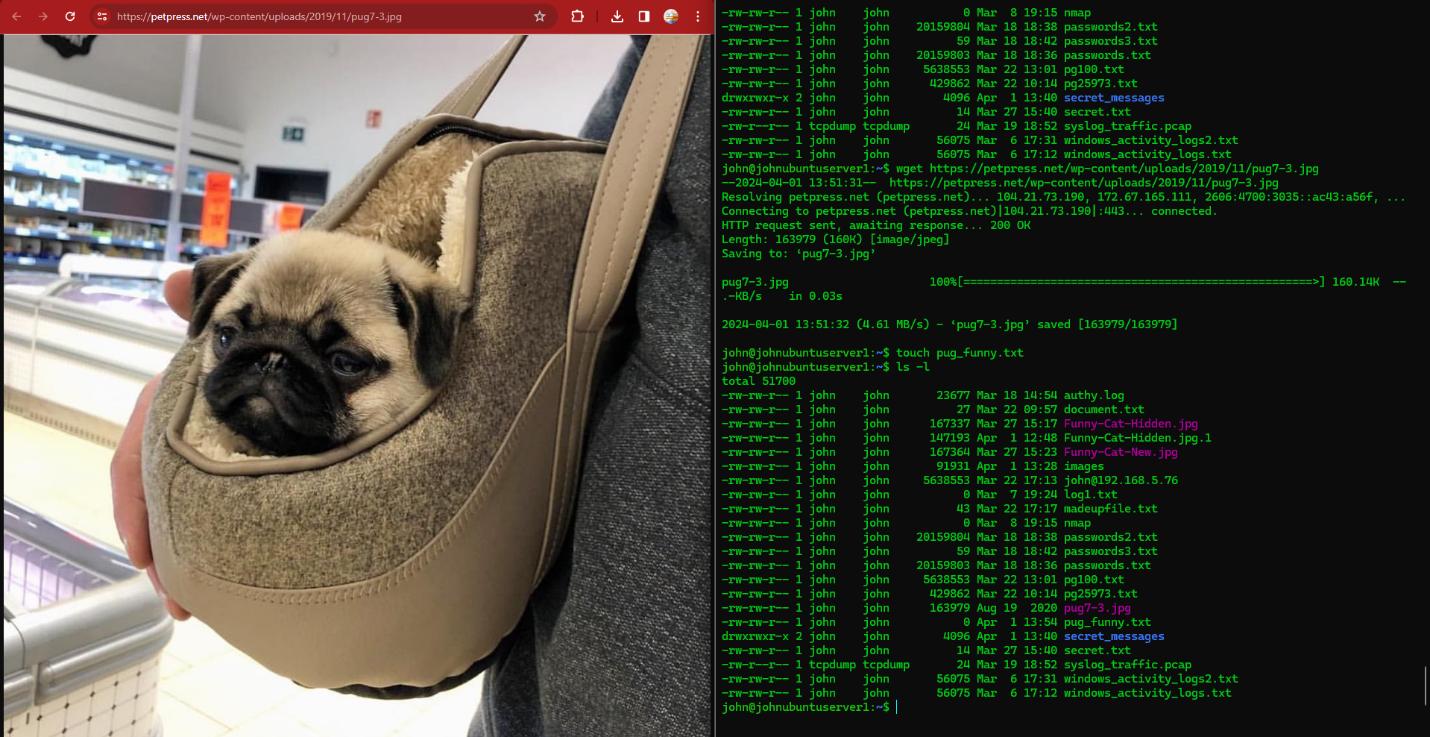
Created Funny-Cat-Hidden-Secret.txt file for Steghide embed file of Funny-Cat-Hidden.jpg using the follow touch Funny-Cat-Hidden-Secret.txt.

Embedded Funny-Cat-Hidden.jpg file using Funny-Cat-Hidden-Secret.txt using the following command Steghide embed -cf Funny-Cat-Hidden.jpg -ef Funny-Cat-Hidden-Secret.txt.

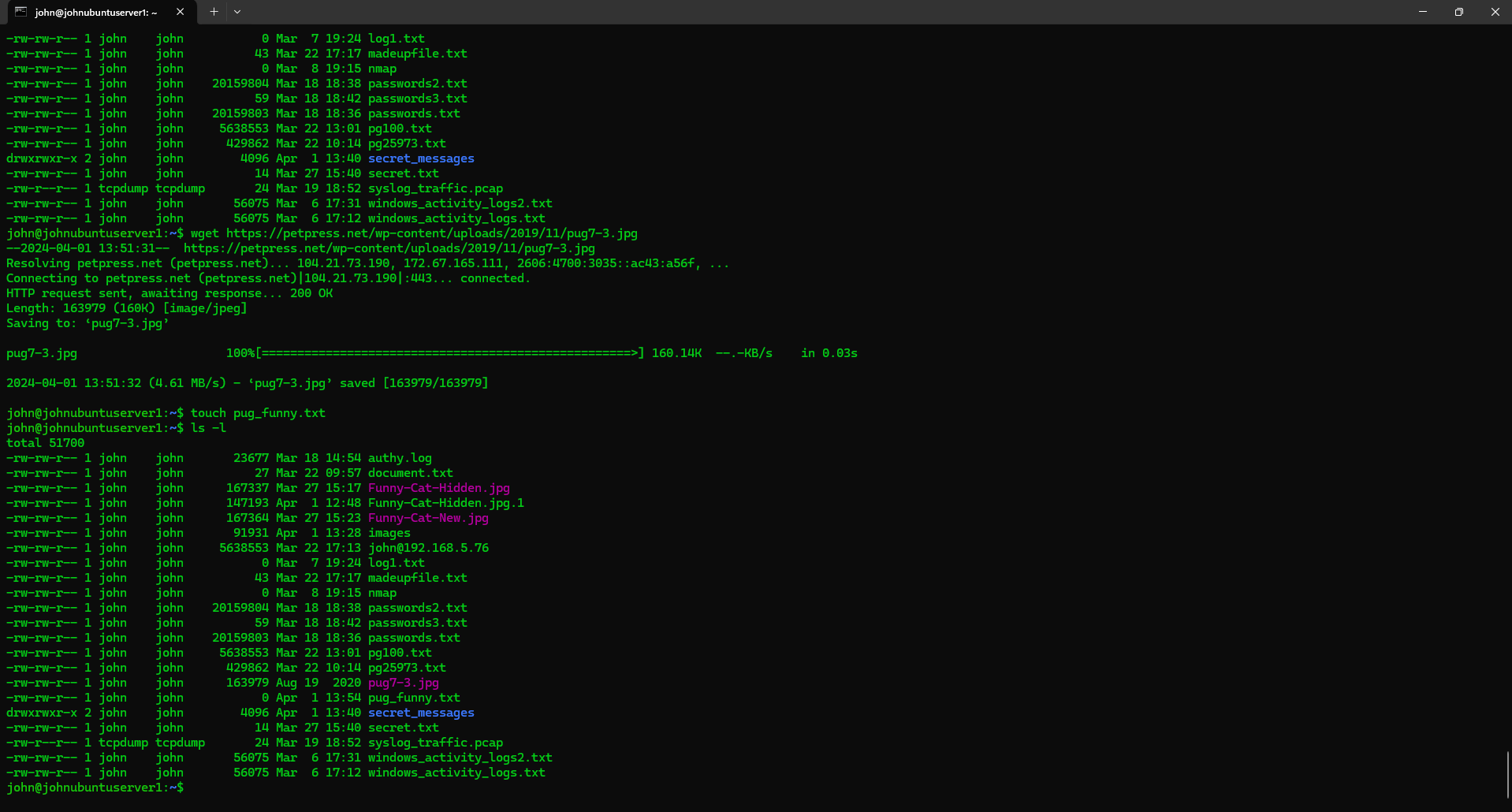
Created A secret message for Funny-Cat-Hidden-Secret.txt using the following command nano Funny-Cat-Hidden-Secret.txt, and then using the nano interface entered: I am more secret now!!, saved file contents and closed nano interface using commands ctrl+o and ctrl+x.



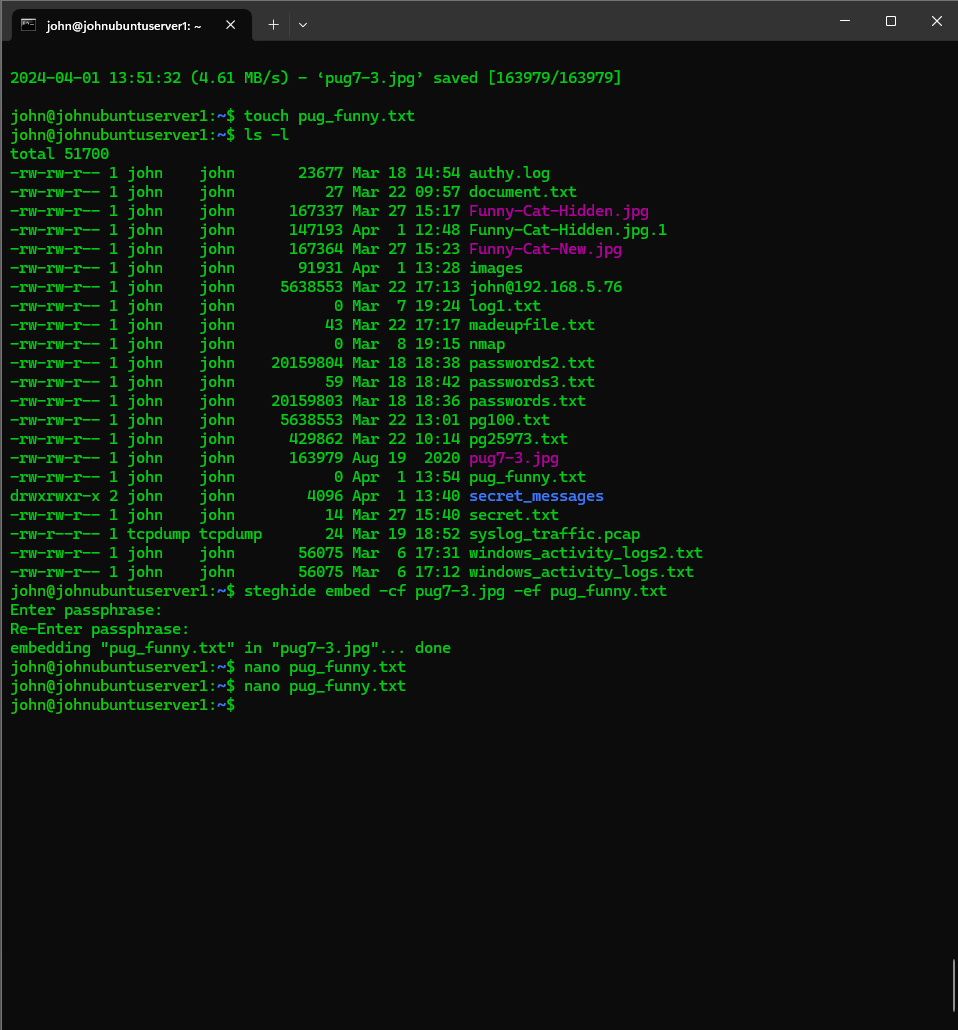
Downloaded pug7-3.jpg to the Linux server using the following command wget https://petpress.net/wp-content/uploads/2019/11/pug7-3.jpg



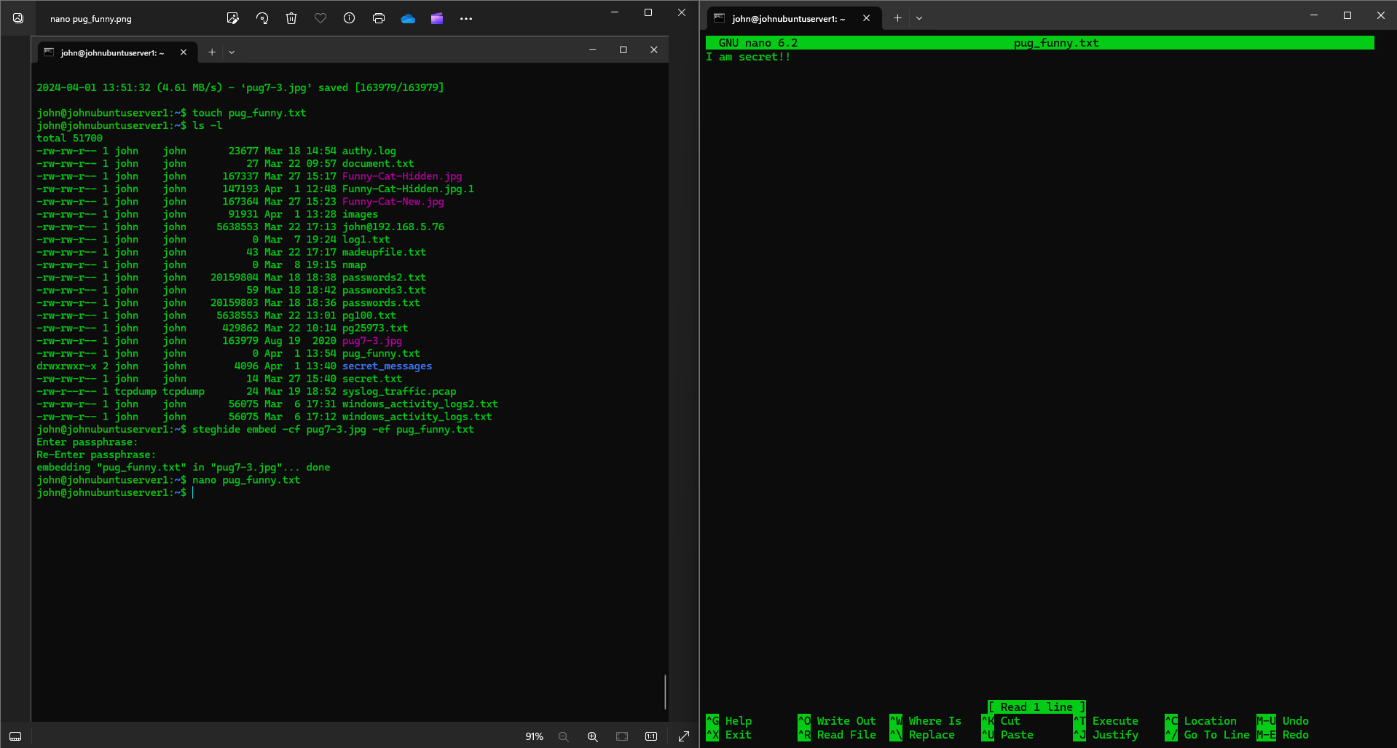
Created pug\_funny.txt file for Steghide embed file of pug7-3.jpg using the follow command touch pug\_funny.txt



Embedded pug7-3.jpg file using pug\_funny.txt using the following command Steghide embed -cf pug7-3.jpg -ef pug\_funny.txt



Created A secret message for pug\_funny.txt using the following command nano pug\_funny.txt, and then using the nano interface entered: I am a secret!!, saved file contents and closed nano interface using commands ctrl+o and ctrl+x.



Task #5-Classmate Data Extraction

RAN OpenStego to extra data from embedded German Shepard image:

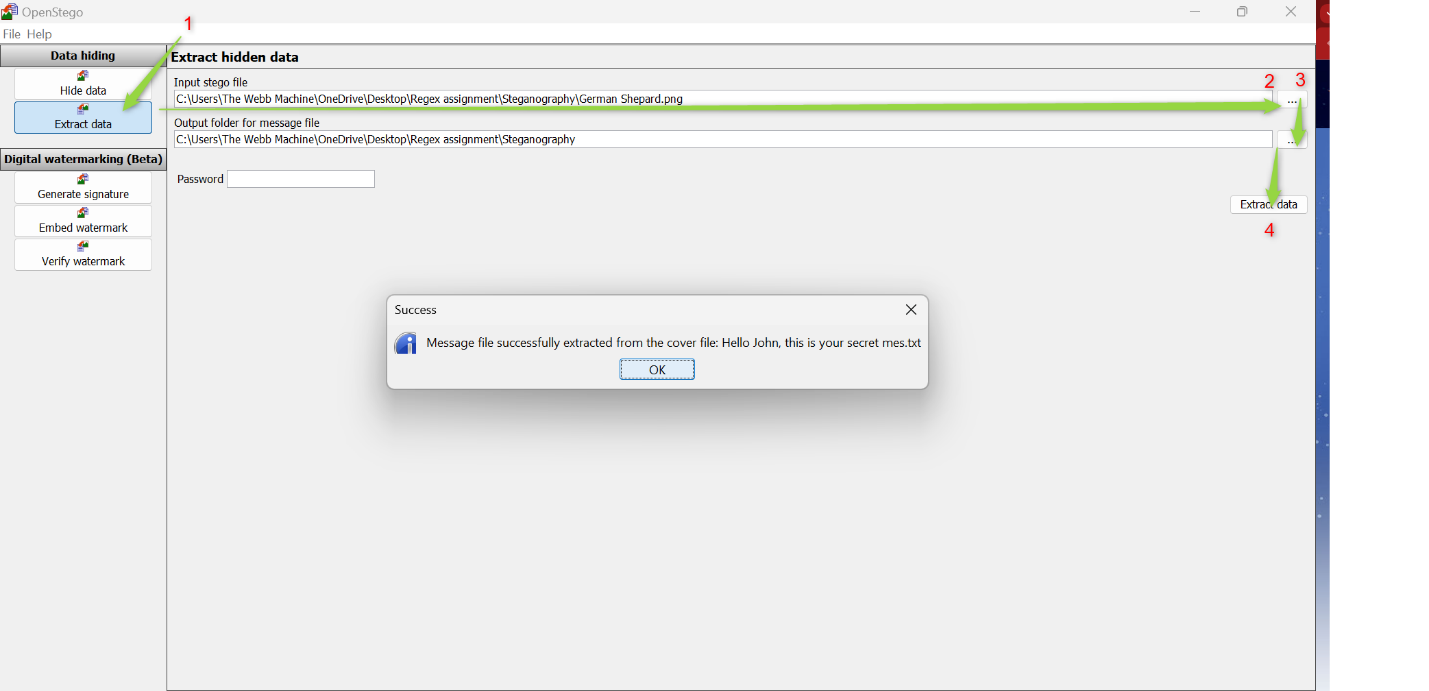


1. Extract Data

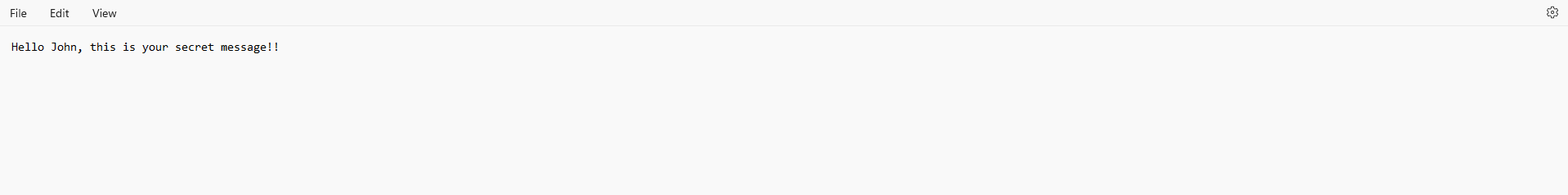
2. Button, select file downloaded

3. Select folder for extraction

4. Click on extract data



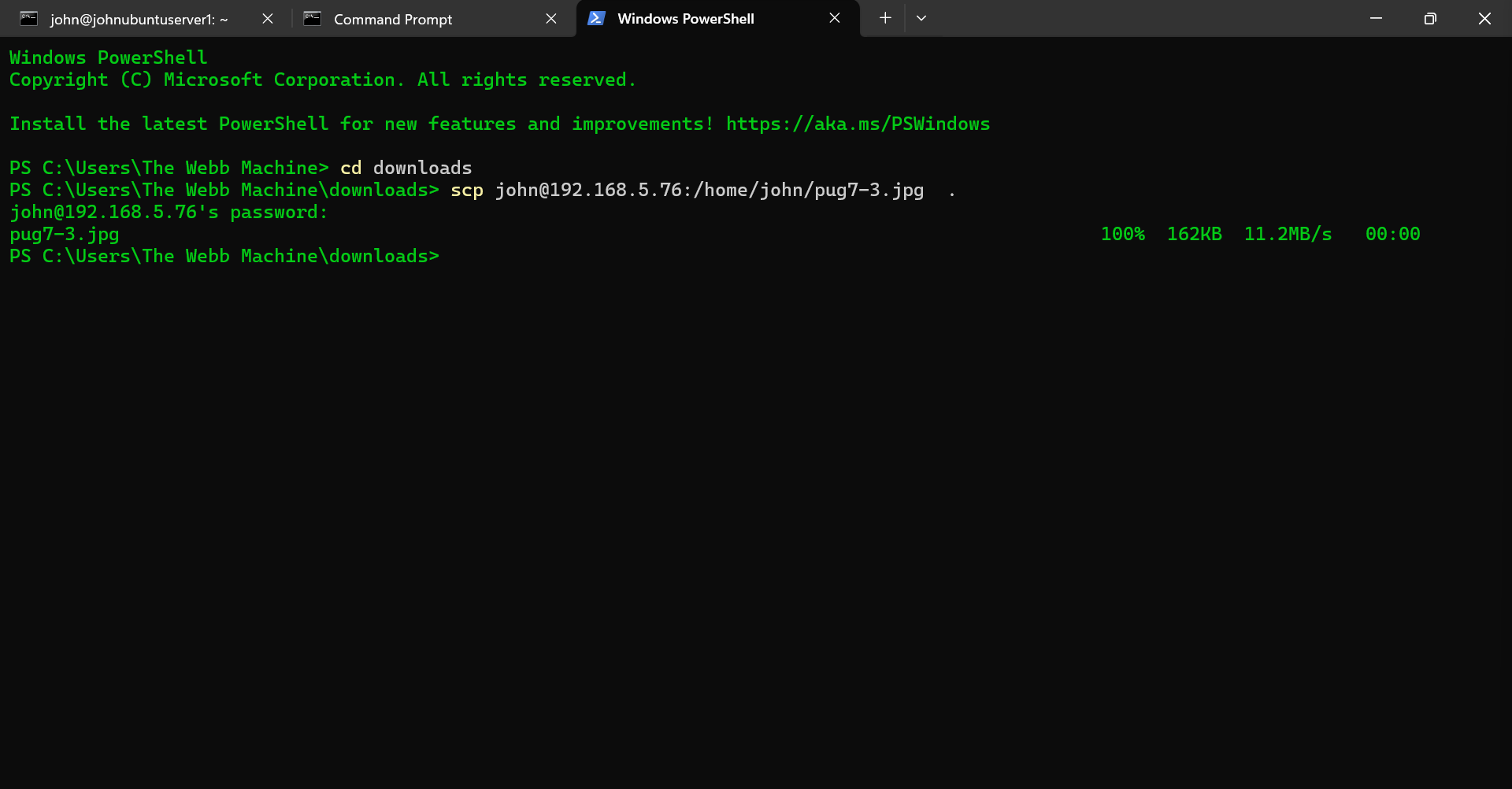
In the Steganography Assignment folder, it will generate the extracted file. Opened the file to read the secret message hidden in the picture:



**Task #3** – Embed a secret into an image

Using Steghide embed a secret into a file & share it with a classmate for them to decode.

I used the pug7-3.jpg file and transferred the file from the Ubuntu Linux server to my host window operating system using the following command: scp john@192.168.5.76:/home/john/pug7-3.jpg.



Downloaded embedded image from a classmate: German-Shepherd-dog-Alsatian

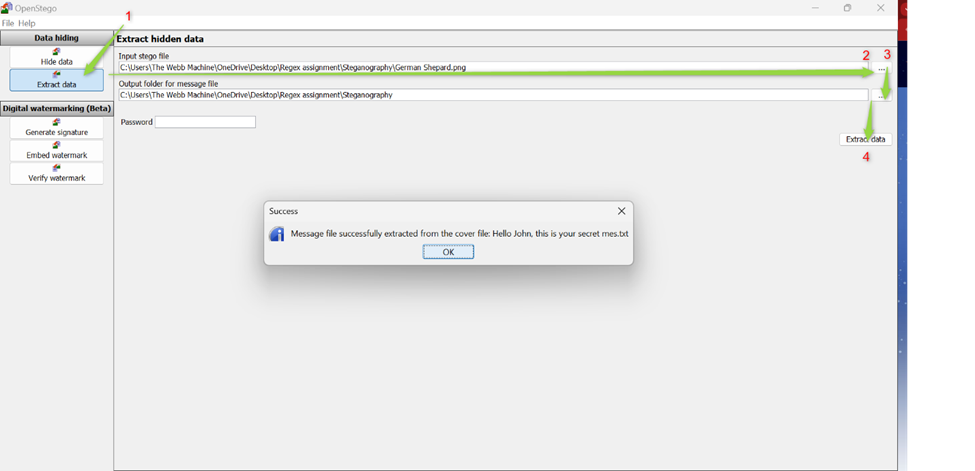


1. Extract Data

2. Button, select file downloaded

3. Select folder for extraction

4. Click on extract data



In the Steganography Assignment folder, it will generate the extracted file. Opened the file to read the secret message hidden in the picture:

