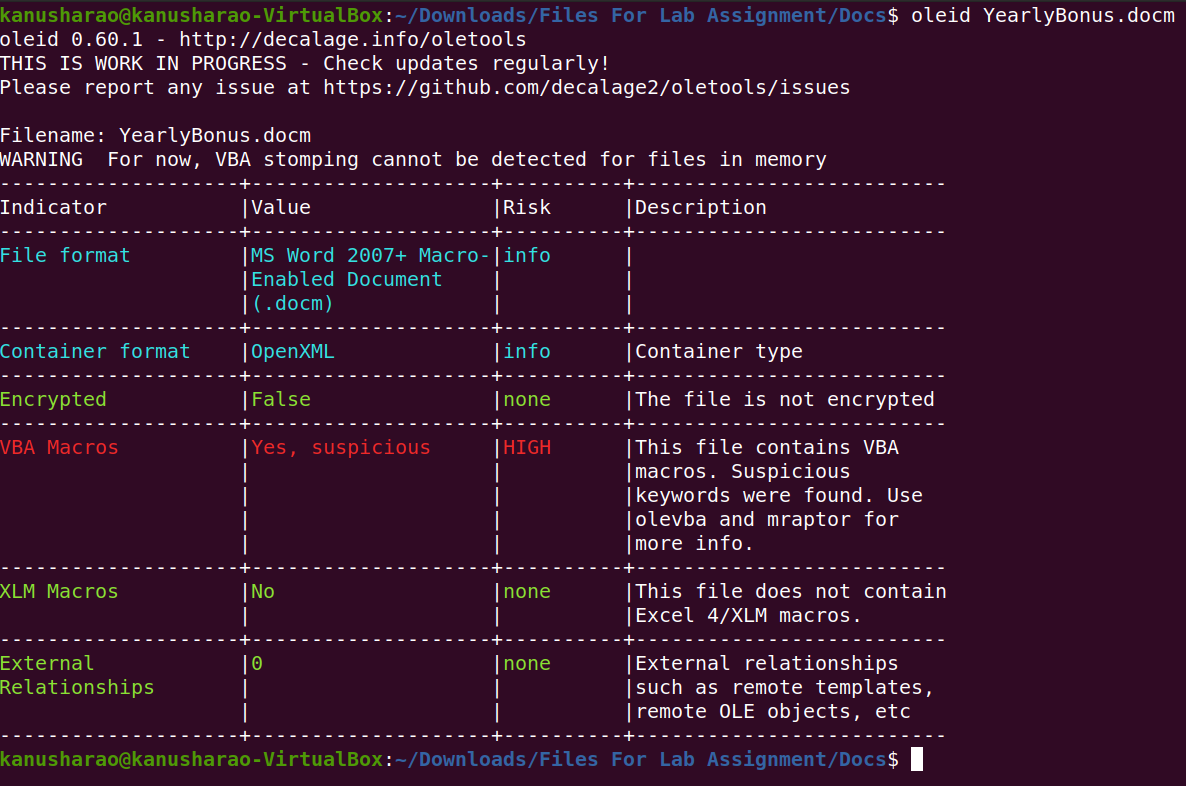
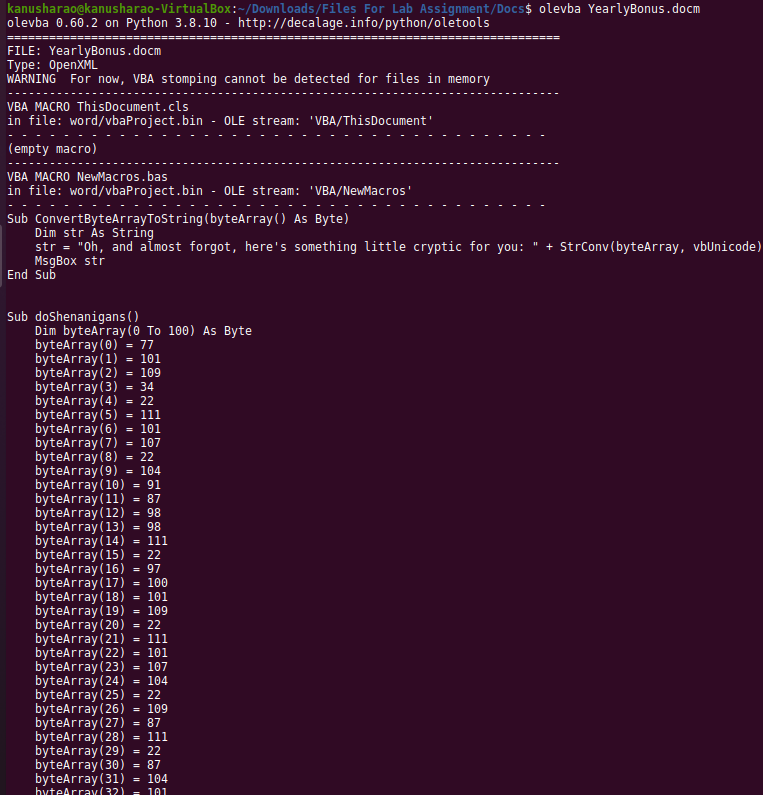
1.A phishing attack has been reported in your organization, where an employee received a malicious Word document in an email that appeared to come from a trusted source. The employee opened the document which had macros in it, resulting in the attacker gaining access to the employee’s computer. A secret which will reveal the attacker's identity, is embedded inside the macro code. You are tasked with analyzing the macro code and extracting the embedded secret. The secret has the format flag{s0me\_str1ng}.

The Word document – Yearly Bonus

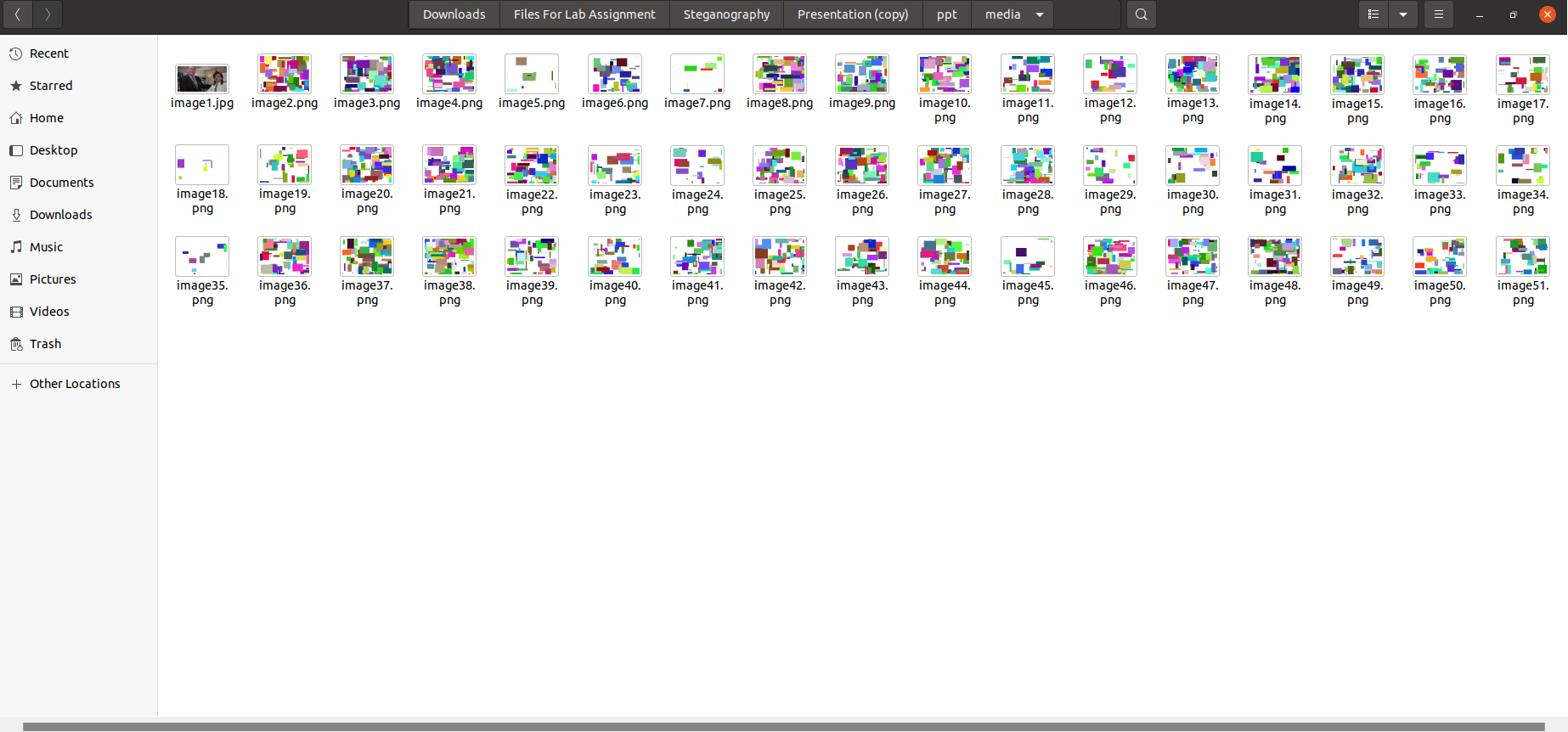
1. Check if macros exist using oleid
2. Getting more info using olevba  
   
3. Byte Array: 77,101,109,34,22,111,101,107,22,104,91,87,98,98,111,22,97,100,101,109,22,111,101,107,104,22,109,87,111,22,87,104,101,107,100,90,22,87,22,76,56,55,22,99,87,89,104,101,22,89,94,87,98,98,91,100,93,91,36,0,0,79,101,107,104,22,92,98,87,93,22,95,105,48,22,92,98,87,93,113,105,107,89,94,85,99,42,89,104,38,85,99,107,89,94,85,109,38,109,23,115
4. With Ceaser cipher 22 shift:   
   7OW YOU REALLY KNOW YOUR WAY AROUND A 6"! MACRO CHALLENGE 9OUR FLAG IS FLAG[SUCH?M CR ?MUCH?W W ]
5. With utf8:

Mem"oekh[WbboademoekhmWoWhekZWL87cWYheY^Wbb[d][$Oekh\bW]\_i0\bW]qikY^Uc\*Yh&UckY^Um&ms

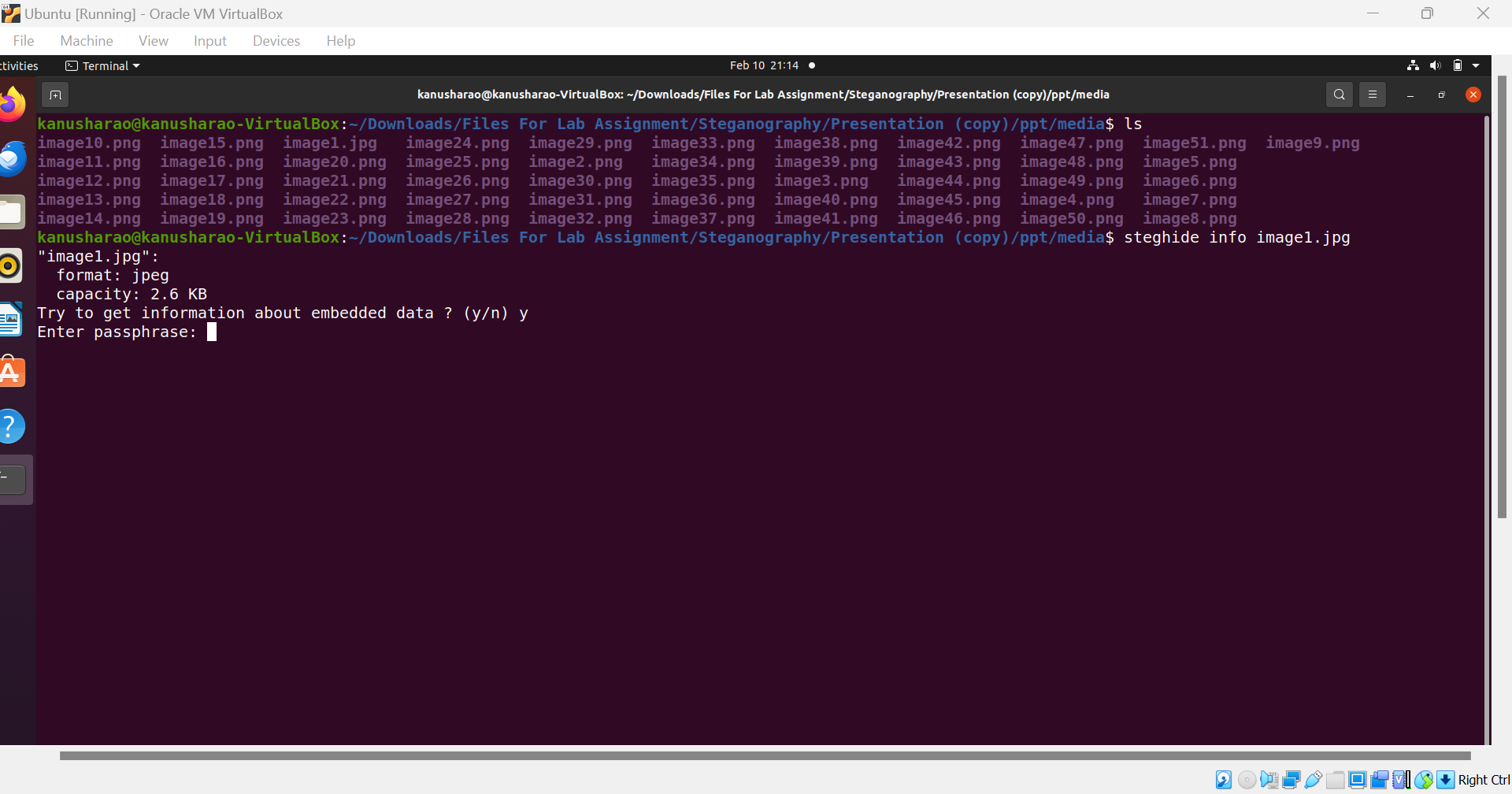
2.A mole within the government has leaked top secret information to a spy. The mole, aware of spycraft techniques, used steganography to hide the information within an image, which he then slipped to his handler. The spy received the image and pasted it into a PowerPoint document, covering it with multiple random images to conceal it. One of our spies has gained access to the enemy spy's computer and recovered the PowerPoint document. Your mission is to extract the first image, extract the top secret information as well as the name and location of his source inside the government.

The PowerPoint document – Presentation.

Created a backup and converted the ppt to zip file and extracted all the files from it

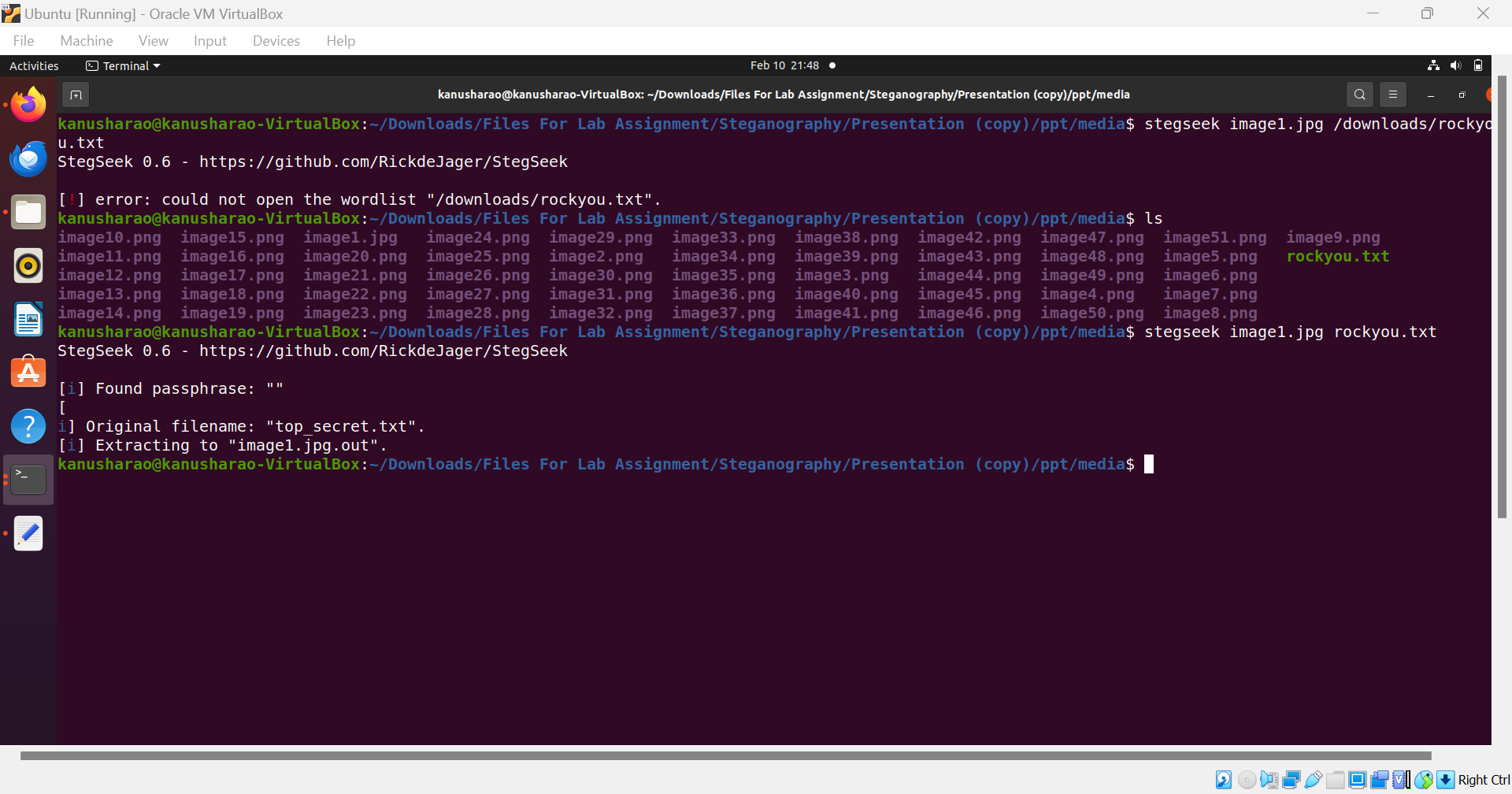


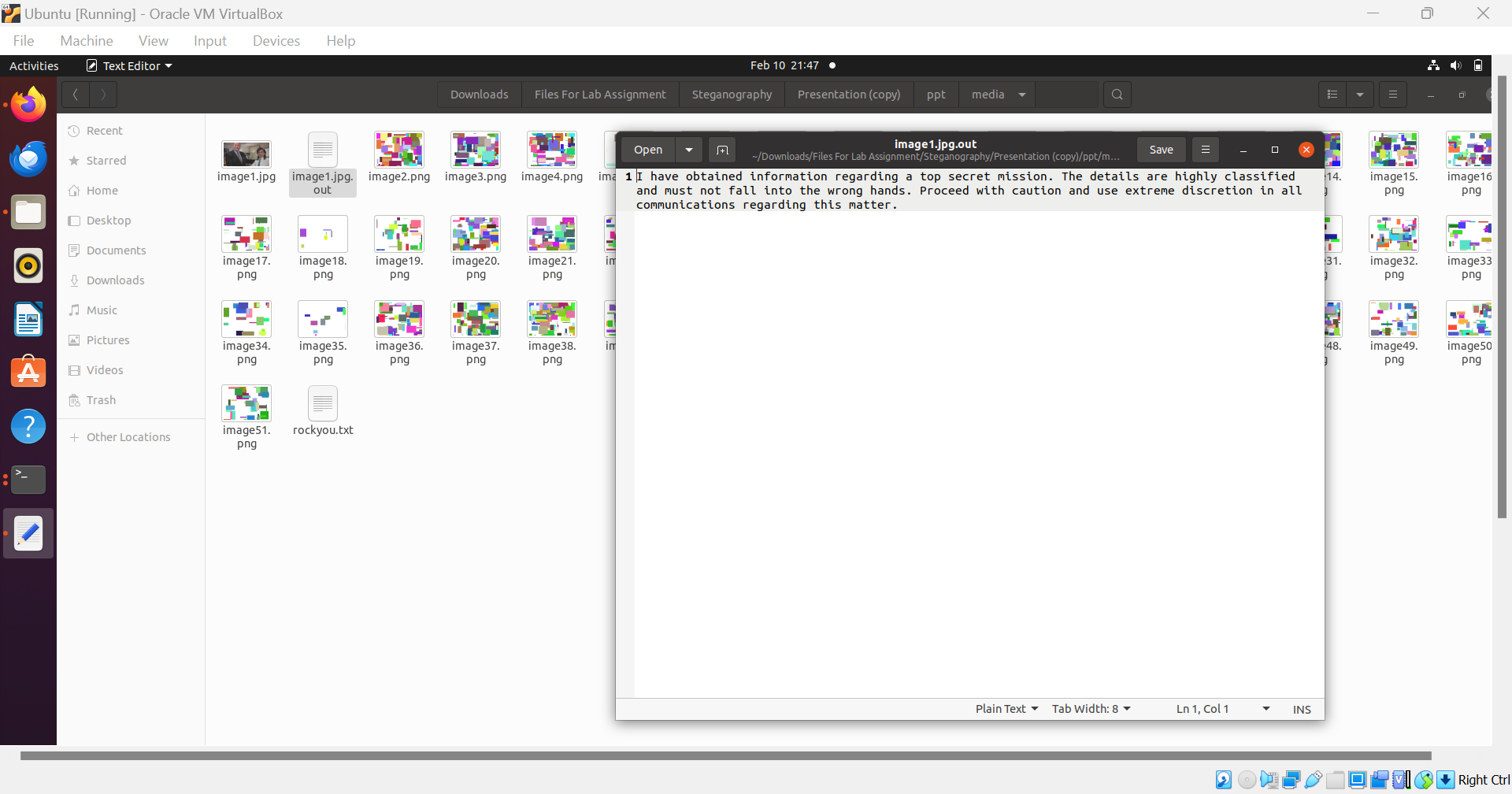
The first image is different from the rest so let me try steghide tool on it



Need a passphrase

Use stegseek to crack the passphrase and extract the hidden content in image





Hidden Message:

I have obtained information regarding a top secret mission. The details are highly classified and must not fall into the wrong hands. Proceed with caution and use extreme discretion in all communications regarding this matter.

Used exiftool to find out more info on the image1.jpg

Artist: Michael Scott

Location:

