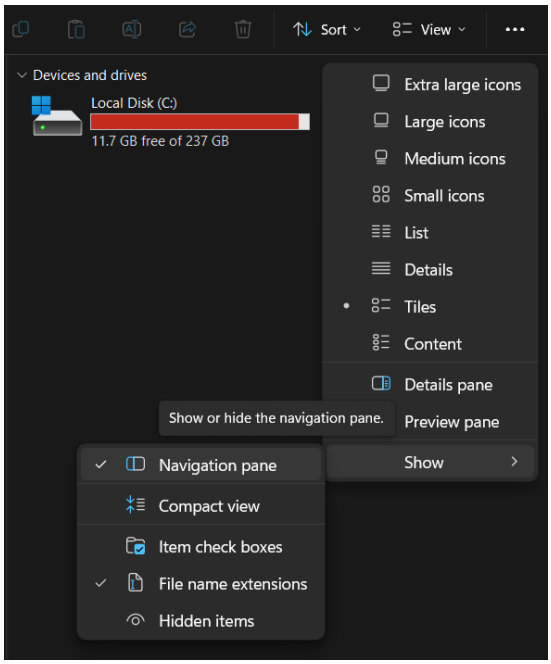
IMPORTANT : Welcome to Amiri's Study Guide for **CIS 152** Finals Checklist. This is not an official guide; I have done my best to compile the information on this course into short step by step tips to avoid the biggest issues with most procedures.

Before we Begin

Check the menus to the right in Windows Server 2019.



Make sure **File Name Extensions** is checked, so you can see the type of files you will be handling!

(Press CTRL + F to search for words in this document.)

If your Mouse gets stuck in a VM, you can get it out by pressing the **R-CTRL Key** until it lets go of your Mouse!

You can share this document using the QR code or

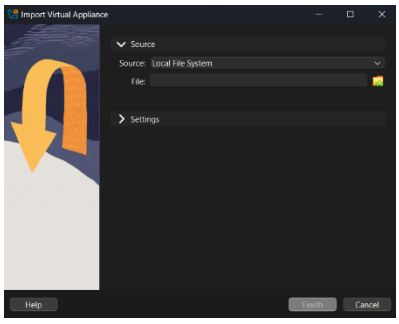
The tinyurl link https://tinyurl.com/Miris152Guide

Section 1: Using Virtual Box

Before you launch a Virtual Machine in Virtual Box (I may also refer to it as **Vbox** for page space)

How to Import a VM

CTRL + i to Import a VM into Virtual Box from a file



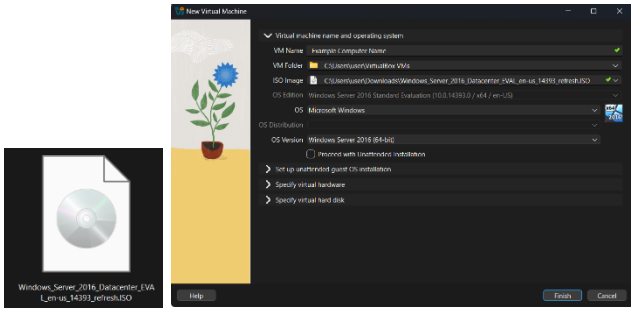
Vbox imports .ova files, find the ones you downloaded, you can see the OVA icon to the right!
Importing a VM is like unpacking a computer when you move.

(Make sure your .ova file is stored on your PC and not in the Network share otherwise it will take forever to start up.)

How to make a VM

CTRL + N to create a VM using from a file

Vbox uses .iso files, find the ones you downloaded, you can see the ISO icon to the right!
This is the **VM creation** menu, you always want to name your VM, include the ISO file
(and unless otherwise specified un-check "Proceed with Unattended Installation")



Using your Vbox

This is the **Right CTRL Key**

(I may also call it the R-CTRL Key) You can use it for a few shortcuts in Virtual Box when your VM is Active!
CTRL + ALT + DELETE to open your Virtual Machine, can also be done with the **Right CTRL Key + Delete Key**

When making a Windows Server Iso file into a VM click the following options :

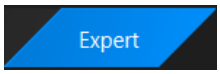
[Next] > [Install Now] > | It is the 2nd option in the menu, NOT the 1st |

[Windows Server 2019 Evaluation (Desktop Experience)] > [I accept the license terms] > [Next] > [Custom: Install Windows Only] > [Next]
and the system should start in 15 minutes or less, and ask you for an Admin password. If this does not happen, delete the VM and try again.

R-CTRL + A makes the window match the size of the VM Screen

R-CTRL + S to open settings, **R-CTRL + Q** to Close your VM

Set up Vbox internal Network

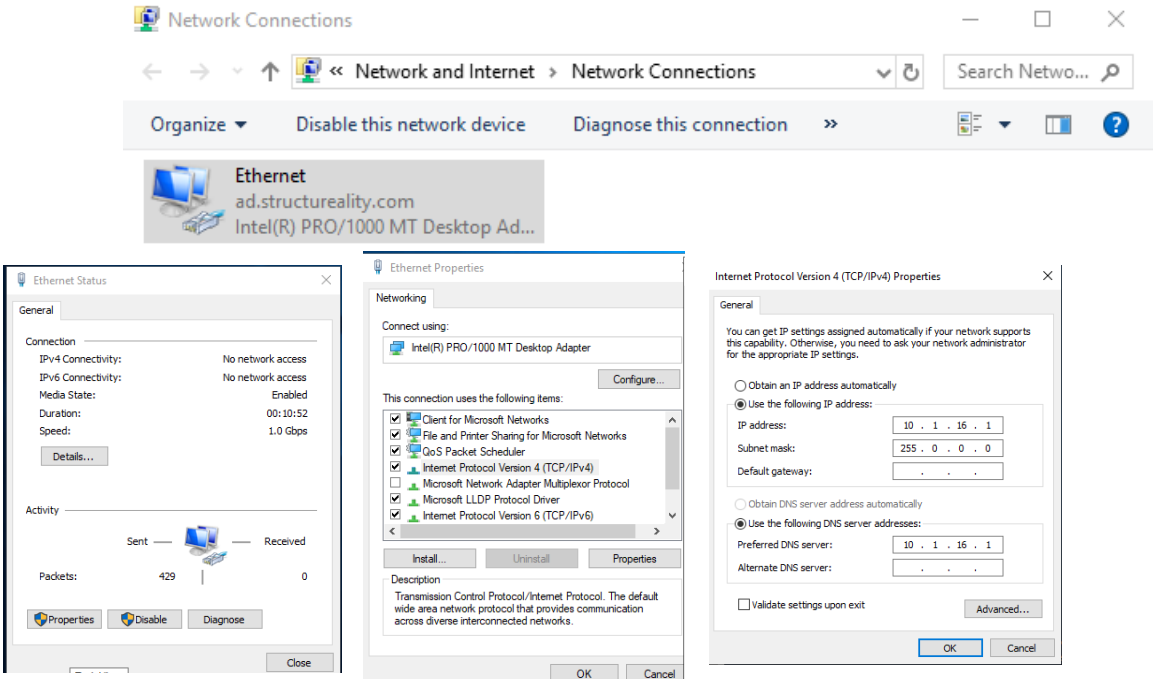
Open your **Vbox settings** to the current VM you are using and make sure to select 

(Continued on Next Page)

Then **Network,** next choose your Adapter 1, Make sure it's enabled, and the drop down for **Attached to** is **Internal Network** (in this mode none of your VMs have internet access but can see each other)

Setting up Ip Addresses

- **In Windows :** There are multiple ways but I'll show you through the **Menus** and through the **CMD**
  - **Windows Menus** : **Windows Key + R** will open the Run menu. If you type **ncpa.pli** and press Enter it will open the Network Connections Menu. From there you can double-click the Network Adapter your VM has (It might be called Ethernet) Then click Properties, and double-click IPV4 you can see the following menus below.

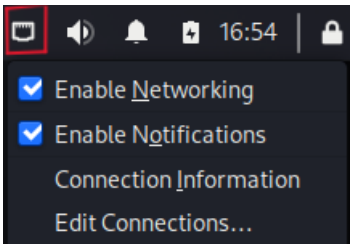


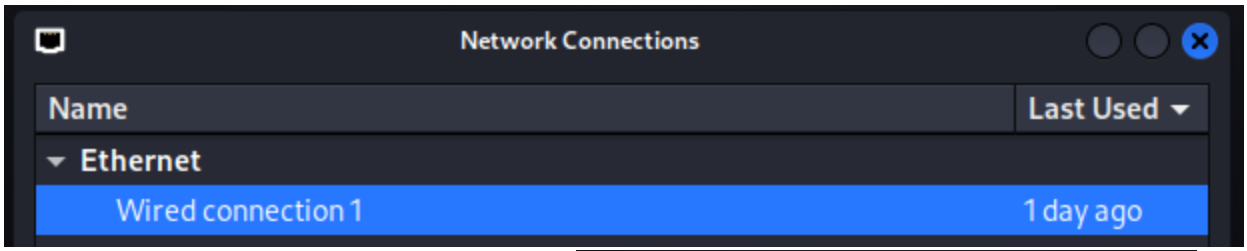
  - **Windows CMD** : Open the start menu and type CMD to open your command line interface. Here is an example of the Windows command to set your IPV4 Address.

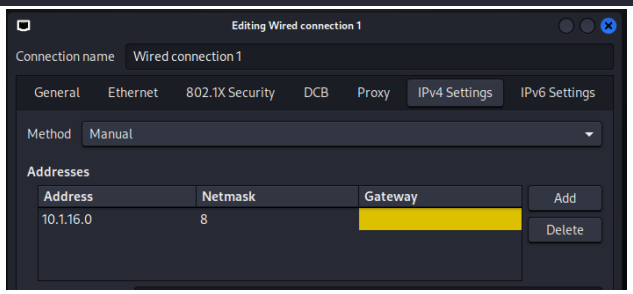
```
netsh interface ipv4 set address name="Wi-Fi" static 10.1.16.1 255.255.255.0 10.1.16.0
```

    - **"Wifi" should be replaced with the name of your Internet/Ethernet Adapter**
    - **10.1.16.1** is the Ip Address for the PC **in this example**
    - **255.255.255.0 example** Subnet Mask (aka /24)
    - **10.1.16.0 example** Gateway

- **In Linux**
  - **Kali Menu** : Once you login look at the top right of the screen where the clock is!
    You will find the "Ethernet Symbol" right click it and this menu will appear under it!
    Select "Edit Connections" and you will be sent to the Connections Menu







Double Click "Wired Connection 1" unless otherwise specified, and in the next menu select IVP4 Settings. Your page should look like this. **DON'T FORGET** to set the Drop down to **Manual** when putting in your IP address (aka not using DHCP) and Click Save.
(If it doesn't work, double check the steps and then restart the VM.)

- **Kali or Metasploitable Linux CLI Command line Interface Code** :
  This is the Code for inputting an IPV4 IP address.

  ```
  sudo ip address add 10.1.16.2/24 dev eth0
  ```

  The way you check if it works is by running it again. Metasploitable should show a message like this `RTNETLINK answers: File exists`

- **IP Addresses in use** – Once you have setup your VMs with a functional Internal Network they should all be able to ping each other. There are no set IP addresses that you have to use in most cases. However in our Checklist the IP Addresses are :

  Windows Server 2019 = **10.1.16.1**
  Kali = **10.1.16.2**
  Metasploitable = **10.1.16.30**

  - During our lessons Professor Chang also uses these Ip Address
    Windows Server 2019 = **192.168.1.100**
    Kali = **192.168.1.150**
    Metasploitable = **192.168.1.200**

Logging In: There are 3 Passwords used for our systems generally. Here they are!
CCPStudent1

Pa55w0rd!

vagrant – for Metaploitable Username and Password (**Metasploitable needs Kali Linux running to start up properly**)

How to use your USB Drive

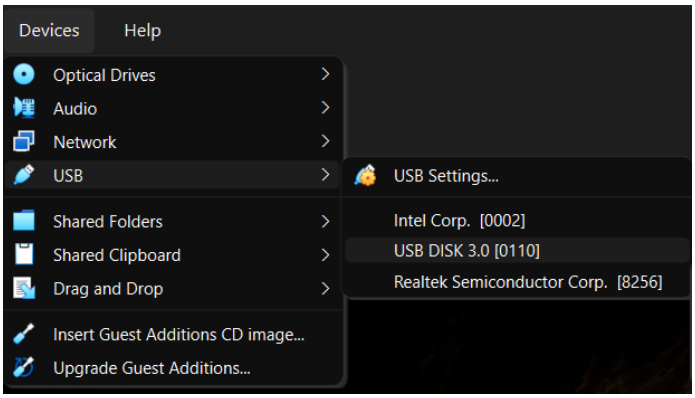
If you remember me insisting everyone bring a USB Drive to the final this is why.

First, you can download any lab files such as CODE https://tinyurl.com/152FinalCode, OS files, and even a copy of this guide!

Secondly, you can use this device to move your files between the host PC and the VM!

In your open VM window, go to the Vbox settings and select **Devices** then **USB.** If you do this before you plug in your USB drive it will show you your computer's internal storage. (You don't want to choose that) Instead plug in your USB drive and select the new option that appears!

(and seems like the name of your drive)



Your drive is now loaded into the VM as if you plugged it in directly!

Simply follow the same steps to **"DeSelect"** the drive and virtually unplug it from the VM.
(If it doesn't show up to your host machine after that just unplug the drive physically and plug it back in, easy peasy.)

(This will work as expected on Windows server 2019 but may require restarting Kali Linux if it does not appear after a few seconds. Although you can use it with Metasploitable, trying to access files through code alone sounds exhausting.)

Using Nmap in Kali Linux

For **Nmap** to run it needs a target. In these examples of code I'll be using **10.1.16.30** as the Target IP

TCP Connect Scan	nmap -sT **10.1.16.30**
Specify Ports to Scan	nmap –p 22,80,443 **10.1.16.30**
Scan a range of ports	nmap -p 1-100 **10.1.16.30**
A basic scan with an XML report in the Home directory	nmap -oX report.xml **10.1.16.30**
An Aggressive Scan with an XML report in the Home directory	nmap -A -oX report.xml **10.1.16.30**

A UDP scan (the rest are TCP)	nmap -sU **10.1.16.30**

PING

the ping command can be used from Windows and Linux with an IP address after it to reach another device. Windows will only send 4 pings when you use the command. Linux will send as many as possible until you press **CTRL + C.**

DoS using **HPING3**

in **Windows Server 2019** Search 🔎 then open the **Performance Monitor**, make sure to click the option under Monitoring Tools. At the bottom you will see % *Processor Time* with a red line. Right-Click and select **Remove All Counters** Right-Click the empty space and select **Add Counter,** it will open a menu and choose **Network Adapter,** then **Packets Received/Sec** and <All instances>

You should see a line that travels up when you run your Hping command (That's your proof that your command is working)

Next from **Kali** send :

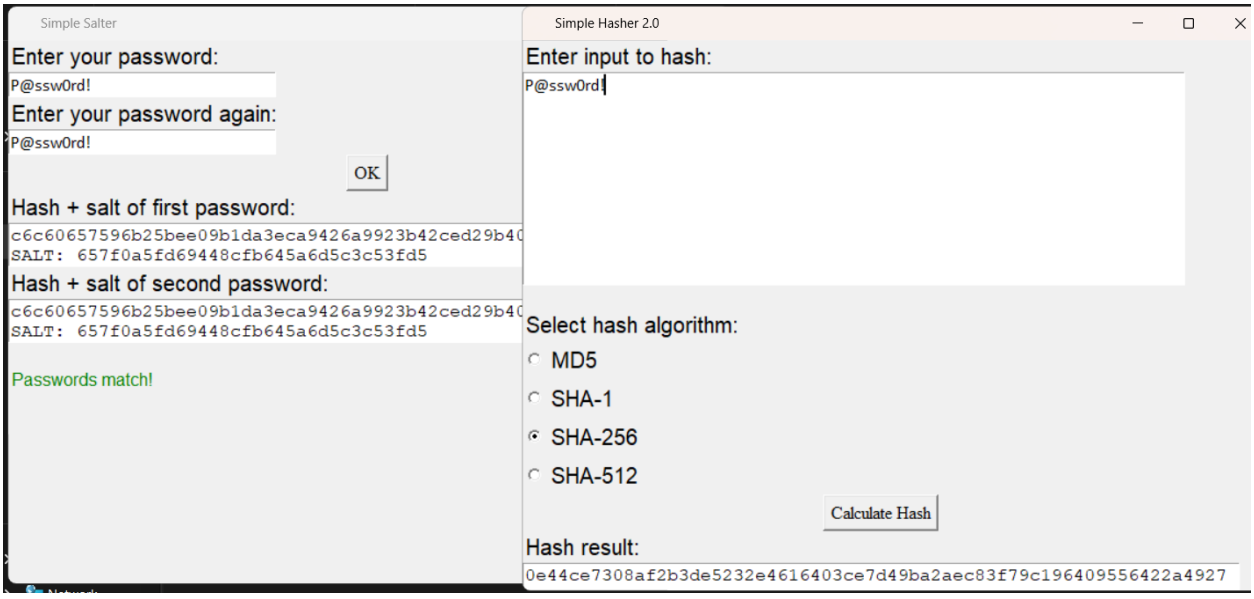
```
hping3 -S -P -U –flood -V –rand-source 192.168.1.100
```

(Make sure your Kali Linux and Windows VMs are connected by Internal Network first)

Salting and Hashing – **Simple Salter.exe** and **Simple Hasher 2.exe** were used in an earlier lab for encrypting information such as passwords.

If they are not preinstalled on your device and you are allowed to access canvas, you can find them in the **Modules tab** for this class in
Week 8/Topic 07: Encryption & Cryptography and download Lab Programs.zip

Both programs are simple enough to use, enter the Password (such as P@ssw0rd!) and run the programs.



ADS (Alternative Data Stream)- an Alternative Data Stream is a feature of the **NTFS file system** in windows, it allows data to be hidden within another file without the file looking bigger. (If you've read Harry Potter think of the magical train station of Platform 1 ¾ . Regardless Here is code that can be used in the command line to create, reveal and remove ADS data.

⚠️ a little note ⚠️ ADS is a feature that is often blocked in Windows to prevent installing hidden malware. If you have access to the original code used in our labs and that works, then please use it. Otherwise after many hours of research I found the code and method that should run on any out of the box copies of Windows Server 2019 without too much trouble.

In this example the file **Host.txt** is used. It is created at the following file path on the computer **C:\Lab\host.txt**. Notepad is used to create the **Data file** that will be hidden within the Host file's location.

You should be able to swap out the Host, file path and text file information to suit whatever you are told to do during the final.

You **WILL** need **both the Command Prompt (aka CMD) AND Windows PowerShell (PShell)** to run commands.

How to Create an ADS txt message

1) First Launch **CMD** as an Admin

This code is how you **make** your **Host file**

```
echo test > C:\Lab\host.txt
```

2. This code will make your **Data file** (Everything you type after **.txt** should be stored within the file itself.)

```
echo test > C:\Lab\data.txt  my example message
```

3.This will copy the data from your **Data file** into the ADS space of your **Host file**

```
type C:\Lab\data.txt > C:\Lab\host.txt:stream
```

4.This is how to check that the new ADS space exists

```
dir /r C:\Lab
```

(Check for a **Host.txt** file and a **Host.txt:stream** file)

5.Now we switch to Windows PowerShell and run this code:

```
type C:\Lab\host.txt:stream
```

The text should be the same as the message you wrote into your **Data** file in the first step.

How to remove hidden ADS data

CMD and PowerShell both have their own variation of this command. Choose whichever feels most comfortable for you!

CMD method

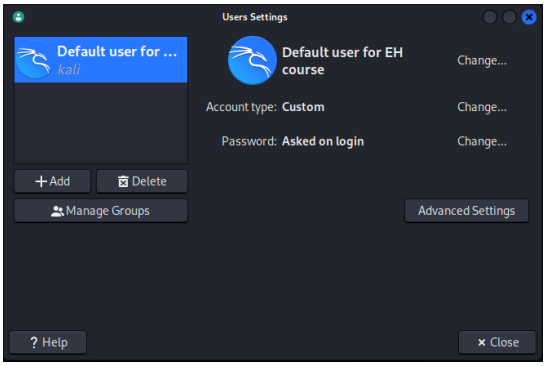
```
fsutil stream delete C:\Lab\host.txt:stream
```

PowerShell Method

```
Remove-Item -Path "C:\Lab\host.txt" -Stream "stream"
```

If you run the command in step 4 the stream file should be gone, and if you run step 5 you should get an error.

Creating Users in Kali Linux



Using Menus : Open the Kali Linux Start Menu, and search for **Users and Groups**, and click the option to open the user menu. Click +Add and then fill out the information. You will need the Kali Linux Password, to make a Username and a Password.

Command Line Interface :

Run **sudo adduser name**. (ensure the name is lowercase).

You will need to answer the following questions

New Password: , Re-type Password: , Full Name :, Room Number: , Work Phone:, Home Phone:. Other, and Confirmation.

Sending an Email

⚠️ a little note ⚠️ To be honest, I'm fairly confused about how to configure the Web Server in Windows 2019 to be a mail server with dns. However, between online resources and notes, these are the codes you should need.

- **Disable the firewall first (In Windows PowerShell)**
  Set-MpPreference -DisableRealtimeMonitoring $false
  (switch $false for $true to re-enable it)

  SC Command Line

  sc config WinDefend start= disabled
  sc stop WinDefend

  or

  sc config WinDefend start= auto
  sc start WinDefend

  (Make sure there is a Space after 'start=')
  (Also **sc/?** or **sc config/?**)

- **Code for Sending an Email from Kali to Windows**

sendemail -f support@ad.structureality.com -t jaime@ad.structureality.com -u "Subject" -m "This is a test email from kali linux" -s 10.1.16.1:25

From :	-f
To :	-t
Subject Line :	-u
Message :	-m

Smtp Server Address + Port Number	-s
Smtp Username	-xu
Smtp Password	-xp

- **Code for sending an Email from Windows (You can also try using Thunderbird)**

  Send-MailMessage -From Cam@ad.structureality.com -To Jaime@ad.structureality.com -Subject "Hello" -Body "Message" -SmtpServer ad.structureality.com

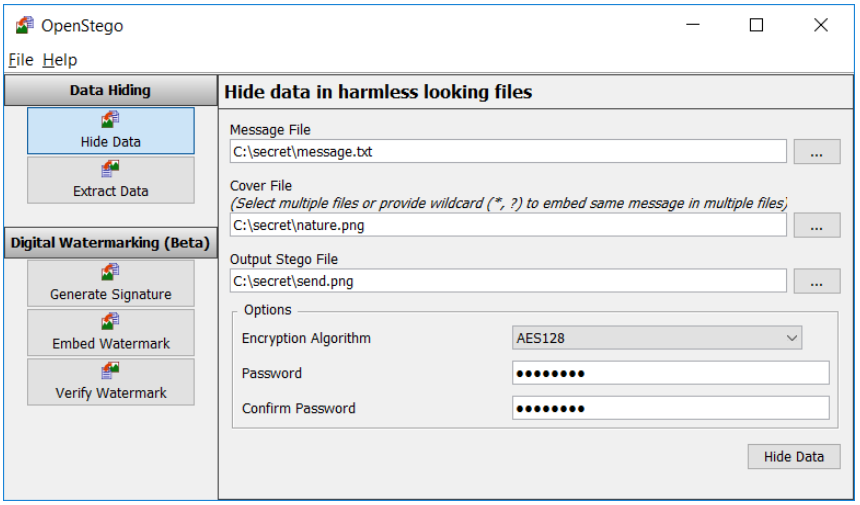
- **Using OpenStego**

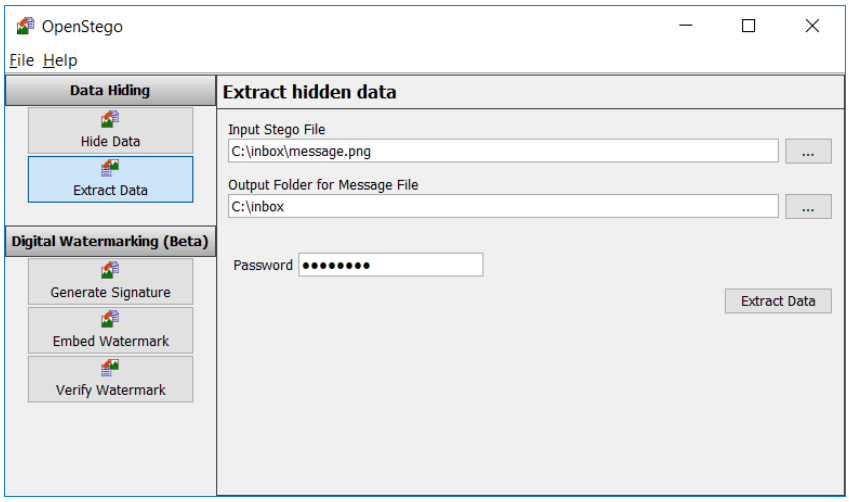
The program has 2 modes, Data Hiding and Data Extracting!

Make sure to load up 2 files, 1 Message file and 1 Cover file.

You can choose your Encryption Algorithm with a password, and use the

Extract Data Feature to see your message again!





Thank you for Reading!

Special Thanks to Jude & the Internet!