CYB102 Project 1

(🔗 Instructions Page)

🧑🏿 Student Name: Didier Joseph DESMANGLES

✉️ Student Email: djdesmangles@gmail.com

Reflection (Required)

> 🤔 **Reflection Question #1:** If I had to **explain "what are .pcap files" in 3 emojis,** they would be... (Feel free to put other comments about your experience in this unit here, too!)
>
> 👁️📄🕵️
> 👁️ The ALL-SEEING-EYE (Wireshark) sees and captures everything that is going on a network to record all the information in a 📄 FILE whom will be examined by 🕵️ The ANALYST..

> 🧠**Reflection Question #2:** How does Wireshark help us to analyze network traffic?
>
> - **Packet Capture (Sniffing)**: Wireshark can intercept and log live data packets moving across a network interface. By capturing packets, users can see the details of each packet, including source and destination addresses, protocols used, and the actual data being transmitted
> - **Protocol Dissection**: This refers to the process of analyzing and interpreting the data packets captured over a network. It involves decoding the various protocols utilized at each layer of the OSI (Open Systems Interconnection) model, allowing for a comprehensive understanding of the data being transmitted.
> - **Detailed analysis**: Wireshark focuses on key components like source and destination IP addresses, port numbers, flags, and payload data
> - **Filtering and Searching**: Filtering and searching capabilities are crucial for efficient traffic analysis. Understanding how to use filters strategically greatly enhances the analysis process, enabling quicker identification of issues.
> - **Visualization**: Wireshark's visualization capabilities empower users to take a proactive approach in managing their networks by providing critical insights into traffic patterns, performance, congestion, and potential threats

> 📢 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

17 - Isael M (Isael MELENDEZ)!!!! <- This dude is AWESOME, humble, and always ready to share !!

Required Challenges (Required)

Item #1: The bad apple's IP address:

192.168.1.4

Item #2: The subject lines of three different phishing emails:

1. You ugly pervert! - rockandrol
   "**Don't Ignore! Confidential Data Exposed!**"

2. You got owned! - maldita
   "**Don't Ignore! Confidential Data Exposed!**"

3. You better read this! - asda123456
   "**Don't Ignore! Confidential Data Exposed!**"

Item #3: An explanation of how you went about finding the bad apple from just the .pcap files: (Please be specific about what filters/searches you used!)

1. **Analyzing all the .pcap**

   1.1. **A.pcap**

   - We apply the Wireshark filter "smtp contains "DATA" to verify whether data (attachment) was transmitted.
   - The Wireshark filter "smtp contains "FROM" allow to verify to source of this attachment. We see IP "**192.168.1.4**" as the source.
   - We export our information as .eml to continue our analysis.
   - We can use the command line tool "**munpack**" to extract all the information from the previous .eml file. We have now 2 files, "part1" (ascii/harmless) and winmail.dat.
   - winmail.dat file in **TNEF** format. We can use "tnef", a linux tool to open the winmail.dat and inspect the content.
   - There are 2 files inside the winmail.dat: packet-tnef-name-string.patch.gz and a png file. We will extract the .gz file to obtain a .patch file.
   - We see that the .patch file looks a lot like C code.

- **Why would C code travel by email ? It is from 192.168.1.4**

1.2. B.pcap

- The Wireshark filter "smtp contains "DATA" and shows only one data transmission.
- The attached files are NEWS.txt and NEWS.txt which have nothing to see with the mail title (SMTP), but the message is still harmless.
- In the other hand, there is an error coming about an "192.168.1.1". It is very different than the enterprise network IP: 10.10.1.4. It looks like an attempt.

1.3. C.pcap

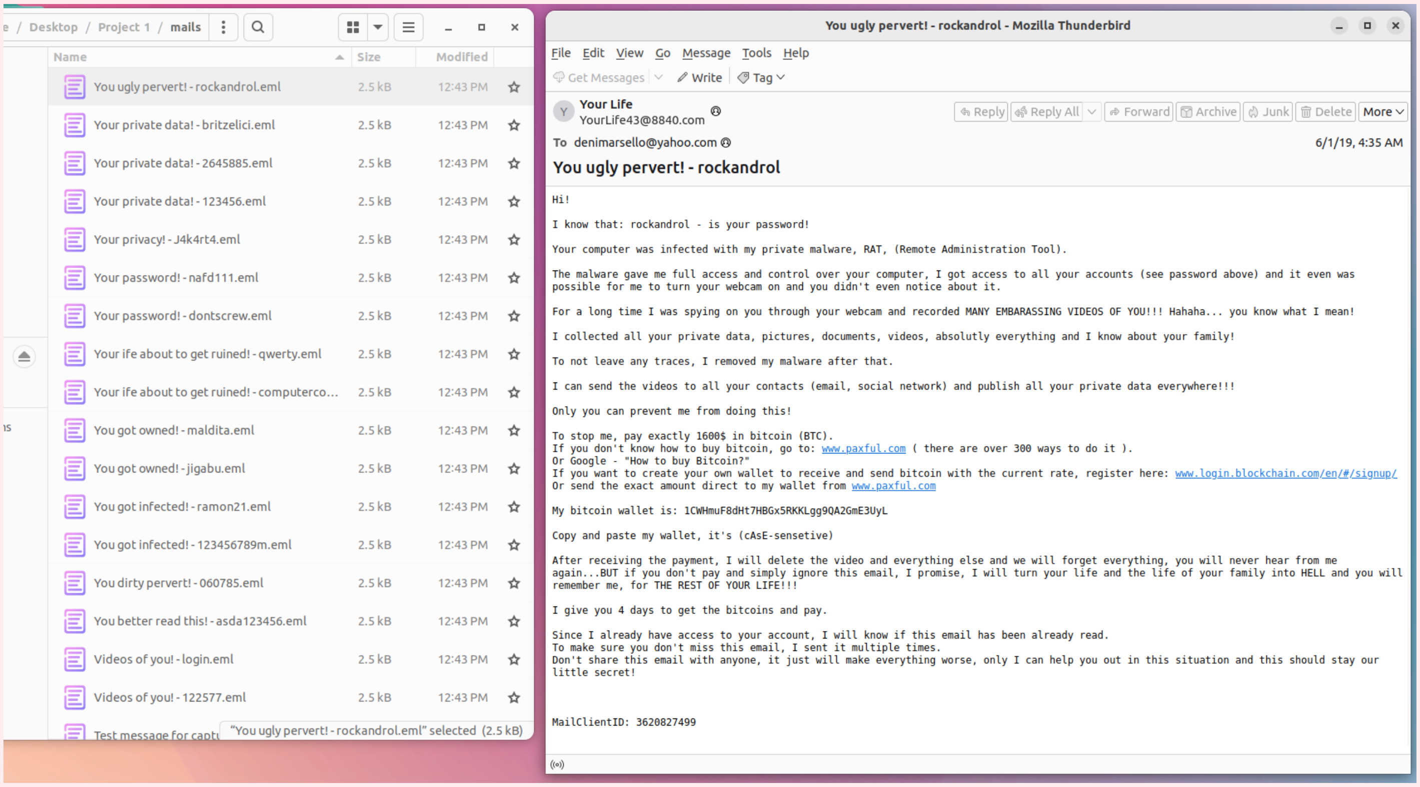
- The c.pcap file contains a capture of the phishing emails. There's no attachment. Only the links are suspect. The IP is different this time: **10.6.1.104.** The mail address in the "FROM" field changes each time but the IP remains the same. Maybe the hacker is using a server to send automatic emails.
- It seems that "awie_sharkawi92@yahoo.com" could be the mail address of the hacker. The error message from the rogue server (pool.washdc.fios.verizon.net) refers to this address.

1.4. D.pcap

- We apply the Wireshark filter "smtp contains "DATA" to verify whether data (attachment) was transmitted. There are "DATA" sent from "**192.168.1.4**" again.
- We follow the procedure and export the information to "*Test message for capture.eml*"
- 3 files are extracted from the .eml with munpack.
  - Words.txt -> This file contains C code !! **WHY ?**
  - words.desc -> is an ascii file. Only contains text.
  - related.patch -> This file also contains a C code apparently designed to attack a LDAP server or an Active Directory.
- THAT comes from **192.168.1.4**

Stretch Challenge (Optional)

> **Item #1:** Three screenshots of three different .eml files showing the content of phishing emails you identified:


e / Desktop / Project 1 / mails
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More

Name	Size	Modified
You ugly pervert! - rockandrol.eml	2.5 kB	12:43 PM
Your private data! - britzelici.eml	2.5 kB	12:43 PM
Your private data! - 2645885.eml	2.5 kB	12:43 PM
Your private data! - 123456.eml	2.5 kB	12:43 PM
Your privacy! - J4k4rt4.eml	2.5 kB	12:43 PM
Your password! - nafd111.eml	2.5 kB	12:43 PM
Your password! - dontscrew.eml	2.5 kB	12:43 PM
Your ife about to get ruined! - qwerty.eml	2.5 kB	12:43 PM
Your ife about to get ruined! - computerco…	2.5 kB	12:43 PM
You got owned! - maldita.eml	2.5 kB	12:43 PM
You got owned! - jigabu.eml	2.5 kB	12:43 PM
You got infected! - ramon21.eml	2.5 kB	12:43 PM
You got infected! - 123456789m.eml	2.5 kB	12:43 PM
You dirty pervert! - 060785.eml	2.5 kB	12:43 PM
You better read this! - asda123456.eml	2.5 kB	12:43 PM
Videos of you! - login.eml	2.5 kB	12:43 PM
Videos of you! - 122577.eml	2.5 kB	12:43 PM
Test message for capt		

“You ugly pervert! - rockandrol.eml” selected (2.5 kB)

You ugly pervert! - rockandrol - Mozilla Thunderbird

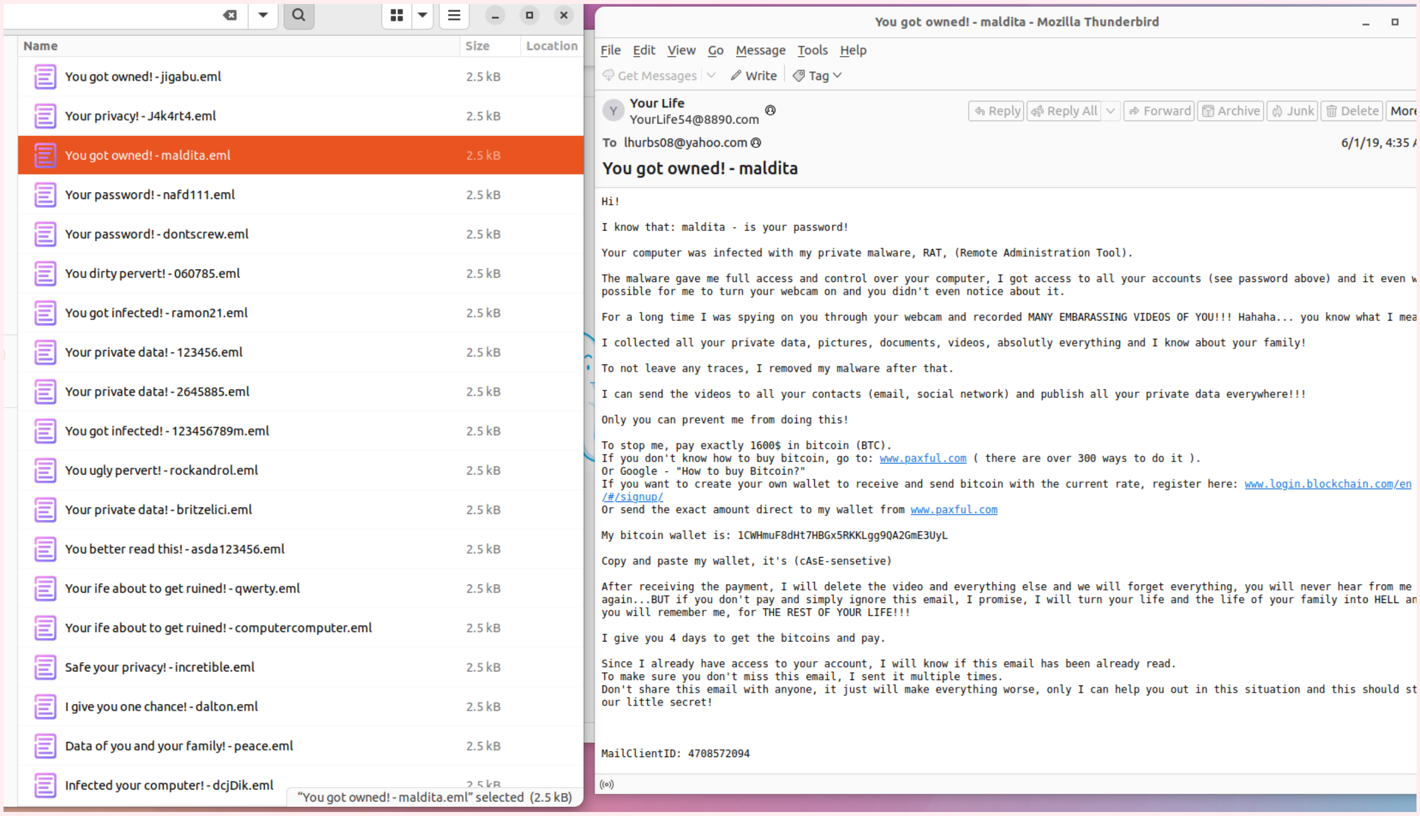
Your Life
YourLife43@8840.com

To denimarsello@yahoo.com

6/1/19, 4:35 AM

You ugly pervert! - rockandrol

```
Hi!

I know that: rockandrol - is your password!

Your computer was infected with my private malware, RAT, (Remote Administration Tool).

The malware gave me full access and control over your computer, I got access to all your accounts (see password above) and it even was
possible for me to turn your webcam on and you didn't even notice about it.

For a long time I was spying on you through your webcam and recorded MANY EMBARASSING VIDEOS OF YOU!!! Hahaha... you know what I mean!

I collected all your private data, pictures, documents, videos, absolutly everything and I know about your family!

To not leave any traces, I removed my malware after that.

I can send the videos to all your contacts (email, social network) and publish all your private data everywhere!!!

Only you can prevent me from doing this!

To stop me, pay exactly 1600$ in bitcoin (BTC).
If you don't know how to buy bitcoin, go to: www.paxful.com ( there are over 300 ways to do it ).
Or Google - "How to buy Bitcoin?"
If you want to create your own wallet to receive and send bitcoin with the current rate, register here: www.login.blockchain.com/en/#/signup/
Or send the exact amount direct to my wallet from www.paxful.com

My bitcoin wallet is: 1CWHmuF8dHt7HBGx5RKKLgg9QA2GmE3UyL

Copy and paste my wallet, it's (cAsE-sensetive)

After receiving the payment, I will delete the video and everything else and we will forget everything, you will never hear from me
again...BUT if you don't pay and simply ignore this email, I promise, I will turn your life and the life of your family into HELL and you will
remember me, for THE REST OF YOUR LIFE!!!

I give you 4 days to get the bitcoins and pay.

Since I already have access to your account, I will know if this email has been already read.
To make sure you don't miss this email, I sent it multiple times.
Don't share this email with anyone, it just will make everything worse, only I can help you out in this situation and this should stay our
little secret!



MailClientID: 3620827499
```



Name	Size	Location
You got owned! - jigabu.eml	2.5 kB	
Your privacy! - J4k4rt4.eml	2.5 kB	
You got owned! - maldita.eml	2.5 kB	
Your password! - nafd111.eml	2.5 kB	
Your password! - dontscrew.eml	2.5 kB	
You dirty pervert! - 060785.eml	2.5 kB	
You got infected! - ramon21.eml	2.5 kB	
Your private data! - 123456.eml	2.5 kB	
Your private data! - 2645885.eml	2.5 kB	
You got infected! - 123456789m.eml	2.5 kB	
You ugly pervert! - rockandrol.eml	2.5 kB	
Your private data! - britzelici.eml	2.5 kB	
You better read this! - asda123456.eml	2.5 kB	
Your ife about to get ruined! - qwerty.eml	2.5 kB	
Your ife about to get ruined! - computercomputer.eml	2.5 kB	
Safe your privacy! - incretible.eml	2.5 kB	
I give you one chance! - dalton.eml	2.5 kB	
Data of you and your family! - peace.eml	2.5 kB	
Infected your computer! - dcjDik.eml	2.5 kB	

“You got owned! - maldita.eml” selected (2.5 kB)

You got owned! - maldita - Mozilla Thunderbird

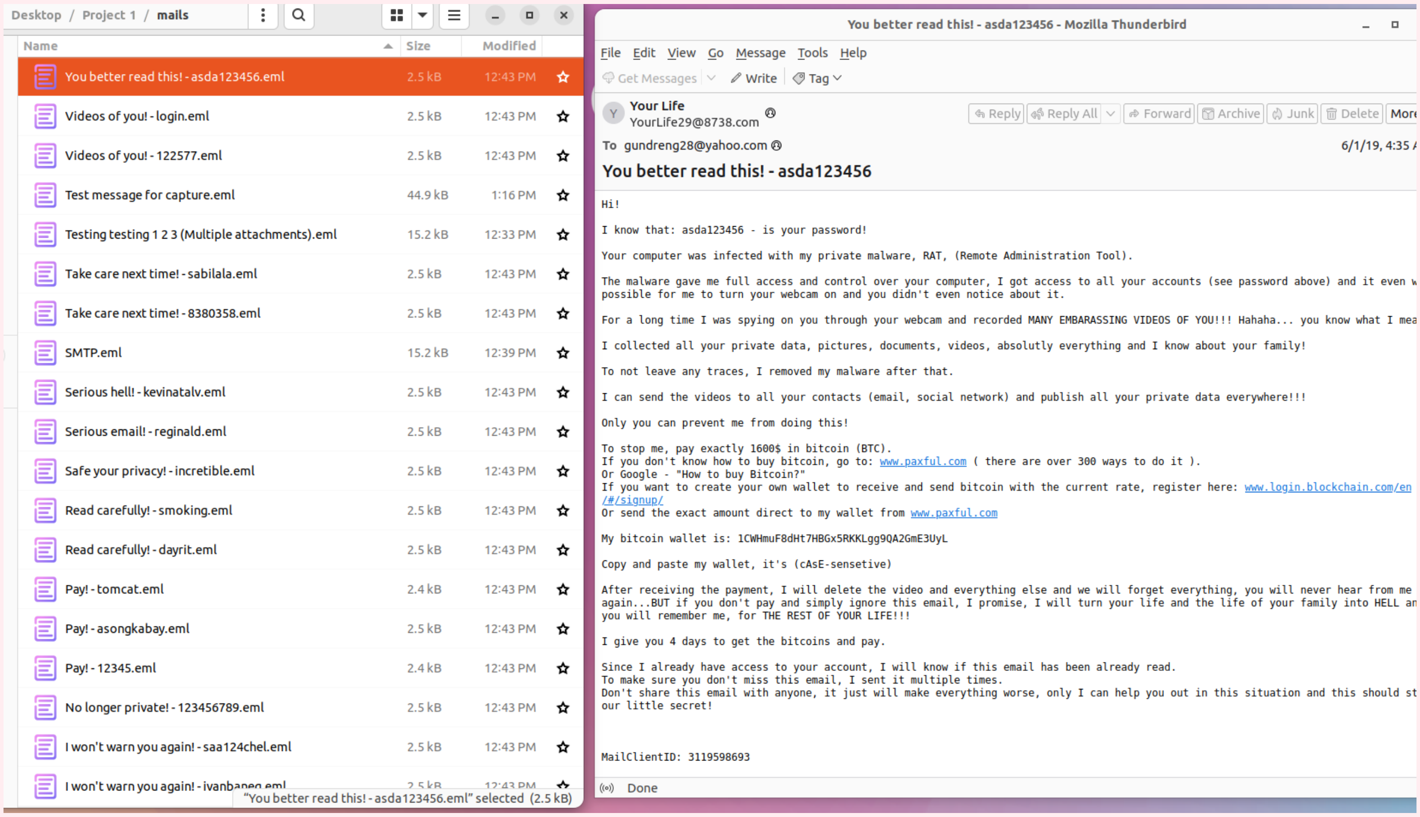
Your Life
YourLife54@8890.com

To lhurbs08@yahoo.com

6/1/19, 4:35

You got owned! - maldita

```
Hi!

I know that: maldita - is your password!

Your computer was infected with my private malware, RAT, (Remote Administration Tool).

The malware gave me full access and control over your computer, I got access to all your accounts (see password above) and it even w
possible for me to turn your webcam on and you didn't even notice about it.

For a long time I was spying on you through your webcam and recorded MANY EMBARASSING VIDEOS OF YOU!!! Hahaha... you know what I mea

I collected all your private data, pictures, documents, videos, absolutly everything and I know about your family!

To not leave any traces, I removed my malware after that.

I can send the videos to all your contacts (email, social network) and publish all your private data everywhere!!!

Only you can prevent me from doing this!

To stop me, pay exactly 1600$ in bitcoin (BTC).
If you don't know how to buy bitcoin, go to: www.paxful.com ( there are over 300 ways to do it ).
Or Google - "How to buy Bitcoin?"
If you want to create your own wallet to receive and send bitcoin with the current rate, register here: www.login.blockchain.com/en
/#/signup/
Or send the exact amount direct to my wallet from www.paxful.com

My bitcoin wallet is: 1CWHmuF8dHt7HBGx5RKKLgg9QA2GmE3UyL

Copy and paste my wallet, it's (cAsE-sensetive)

After receiving the payment, I will delete the video and everything else and we will forget everything, you will never hear from me
again...BUT if you don't pay and simply ignore this email, I promise, I will turn your life and the life of your family into HELL an
you will remember me, for THE REST OF YOUR LIFE!!!

I give you 4 days to get the bitcoins and pay.

Since I already have access to your account, I will know if this email has been already read.
To make sure you don't miss this email, I sent it multiple times.
Don't share this email with anyone, it just will make everything worse, only I can help you out in this situation and this should st
our little secret!



MailClientID: 4708572094
```


Desktop / Project 1 / mails
You better read this! - asda123456 - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More
Done

Name	Size	Modified	
You better read this! - asda123456.eml	2.5 kB	12:43 PM	☆
Videos of you! - login.eml	2.5 kB	12:43 PM	☆
Videos of you! - 122577.eml	2.5 kB	12:43 PM	☆
Test message for capture.eml	44.9 kB	1:16 PM	☆
Testing testing 1 2 3 (Multiple attachments).eml	15.2 kB	12:33 PM	☆
Take care next time! - sabilala.eml	2.5 kB	12:43 PM	☆
Take care next time! - 8380358.eml	2.5 kB	12:43 PM	☆
SMTP.eml	15.2 kB	12:39 PM	☆
Serious hell! - kevinatalv.eml	2.5 kB	12:43 PM	☆
Serious email! - reginald.eml	2.5 kB	12:43 PM	☆
Safe your privacy! - incretible.eml	2.5 kB	12:43 PM	☆
Read carefully! - smoking.eml	2.5 kB	12:43 PM	☆
Read carefully! - dayrit.eml	2.5 kB	12:43 PM	☆
Pay! - tomcat.eml	2.4 kB	12:43 PM	☆
Pay! - asongkabay.eml	2.5 kB	12:43 PM	☆
Pay! - 12345.eml	2.4 kB	12:43 PM	☆
No longer private! - 123456789.eml	2.5 kB	12:43 PM	☆
I won't warn you again! - saa124chel.eml	2.5 kB	12:43 PM	☆
I won't warn you again! - ivanbaneg.eml	2.5 kB	12:43 PM	☆

"You better read this! - asda123456.eml" selected (2.5 kB)

Your Life
YourLife29@8738.com

To gundreng28@yahoo.com

6/1/19, 4:35

You better read this! - asda123456

```
Hi!

I know that: asda123456 - is your password!

Your computer was infected with my private malware, RAT, (Remote Administration Tool).

The malware gave me full access and control over your computer, I got access to all your accounts (see password above) and it even w
possible for me to turn your webcam on and you didn't even notice about it.

For a long time I was spying on you through your webcam and recorded MANY EMBARASSING VIDEOS OF YOU!!! Hahaha... you know what I mea

I collected all your private data, pictures, documents, videos, absolutly everything and I know about your family!

To not leave any traces, I removed my malware after that.

I can send the videos to all your contacts (email, social network) and publish all your private data everywhere!!!

Only you can prevent me from doing this!

To stop me, pay exactly 1600$ in bitcoin (BTC).
If you don't know how to buy bitcoin, go to: www.paxful.com ( there are over 300 ways to do it ).
Or Google - "How to buy Bitcoin?"
If you want to create your own wallet to receive and send bitcoin with the current rate, register here: www.login.blockchain.com/en
/#/signup/
Or send the exact amount direct to my wallet from www.paxful.com

My bitcoin wallet is: 1CWHmuF8dHt7HBGx5RKKLgg9QA2GmE3UyL

Copy and paste my wallet, it's (cAsE-sensetive)

After receiving the payment, I will delete the video and everything else and we will forget everything, you will never hear from me
again...BUT if you don't pay and simply ignore this email, I promise, I will turn your life and the life of your family into HELL an
you will remember me, for THE REST OF YOUR LIFE!!!

I give you 4 days to get the bitcoins and pay.

Since I already have access to your account, I will know if this email has been already read.
To make sure you don't miss this email, I sent it multiple times.
Don't share this email with anyone, it just will make everything worse, only I can help you out in this situation and this should st
our little secret!



MailClientID: 3119598693
```

Notes (Optional): I just installed Thunderbird to open the eml files.

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

Required Challenges

- ~~Item #1~~
- ~~Item #2~~
- ~~Item #3~~

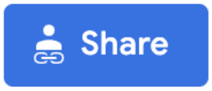
Stretch Challenge

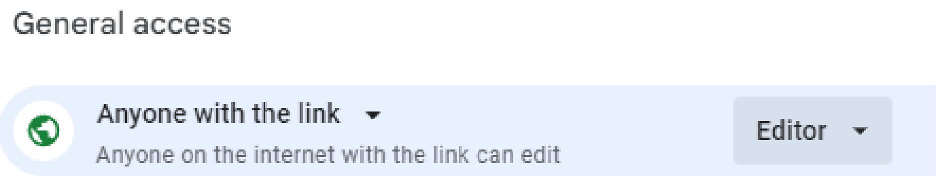
- ~~Item #1~~

💡***Tip: You can see specific grading information, including points breakdown, by going to*** 🔗 ***the grading page on the course portal.***

Submit your work!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit.





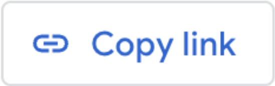
General access

Anyone with the link

Anyone on the internet with the link can edit

Editor

Step 2: **Copy** the link to this document.



Step 3: **Submit** the link on the portal.