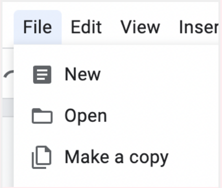
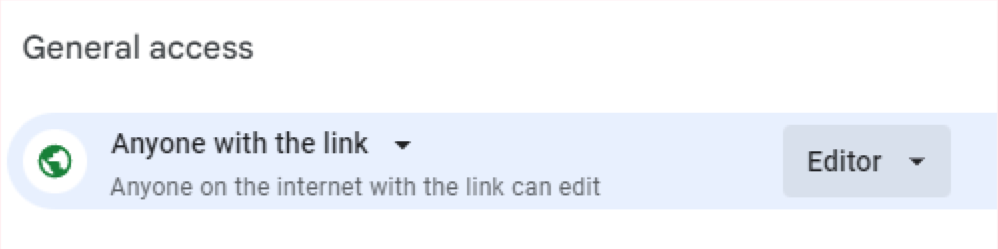
Instructions for Copying and Sharing this Document
📣 **DELETE THIS BOX BEFORE SUBMITTING!!**

Step 1: **Click** “File -> Make a Copy” to make a copy of this document that you can edit.



Step 2: **Change** the Share settings to “Anyone with Link -> Editor”. This will allow our graders to leave comments on your submission.


General access

Anyone with the link

Anyone on the internet with the link can edit

Editor

CYB102 Project 1 (🔗 [Instructions Page](#))

👤 Student Name: Devin Khun
✉️ Student Email: khundevin@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!)
>
> If I had to describe .pcap files, which are used to capture and store network traffic data, the three emojis I would use are: 🌐, 📊, and 📁.
>
> - 🌐 (Globe): Represents the interconnected network traffic between the client and servers
> - 📊 (Bar Chart): Indicates analyzing and inspecting packet data

- 📁 (File Folder): Represents the data stored within the network traffic

.pcap files are essential for network analysis because they provide a raw view of the network traffic passing through a network. This is crucial for understanding communication, troubleshooting issues, and cybersecurity forensic analysis. Observing and analyzing these files helps better understand what is happening on the network beyond surface-level metrics.

🧠**Reflection Question #2:** How does Wireshark help us to analyze network traffic?

Wireshark is a powerful tool for analyzing network traffic because it allows you to capture, view, and interpret the data being transmitted over a network in real time or from recorded files. Wireshark captures raw network traffic and records all packets sent and received on a network during a specified time frame. It includes display filters to identify specific protocols, such as HTTP, TCP, and DNS. Wireshark breaks down packet data into understandable fields, such as IP addresses, port numbers, flags, and headers, for easier packet analysis. During a Wireshark capture, you can monitor ongoing network traffic in real-time, which is useful for detecting unauthorized activity and malware.

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

Shoutout to Group 26 and Tech Fellow Jacob Lapin!

Required Challenges (Required)

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

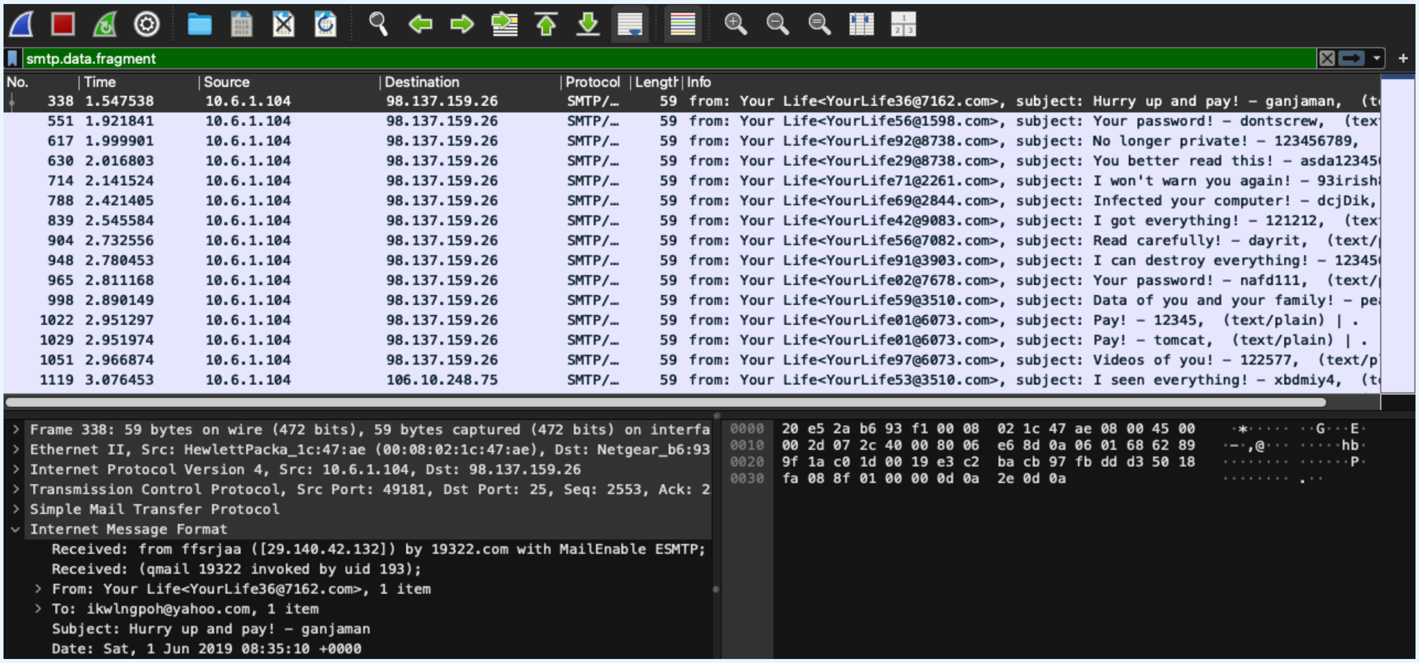
10.6.1.104

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

1. **Hurry up and pay! - ganjaman**
2. **Your private data! - britzelici**
3. **Your password! - dontscrew**

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!)

Initially, I did a quick scan of all four .pcap capture files to see what kind of packets were captured during each time frame. I noticed that the C.pcap files had a lot more packet data using the SMTP protocol, which is used for email messages over the internet. Having looked online at the [Wireshark Display Filter Reference](), I found out that the content of emails is sent in data fragments. I was able to find the malicious actor's IP address by applying the display filter, "smtp.data.fragment", and saw that the source IP address 10.6.1.104 was sending multiple phishing emails.



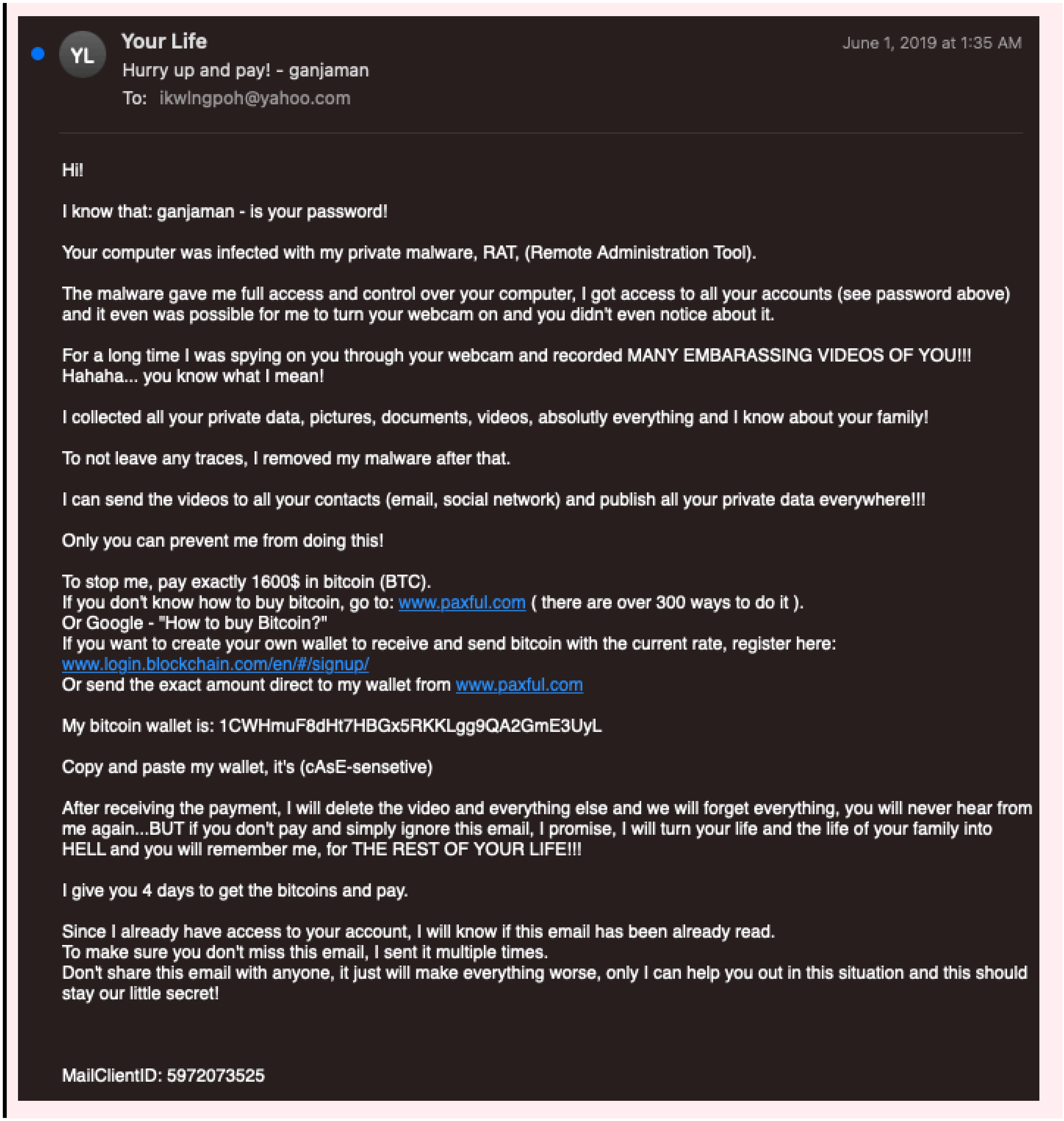
```
smtp.data.fragment
No.    Time      Source      Destination     Protocol Length Info
  338 1.547538  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife36@7162.com>, subject: Hurry up and pay! – ganjaman,  (t
  551 1.921841  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife56@1598.com>, subject: Your password! – dontscrew,  (tex
  617 1.999901  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife92@8738.com>, subject: No longer private! – 123456789,
  630 2.016803  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife29@8738.com>, subject: You better read this! – asda12345
  714 2.141524  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife71@2261.com>, subject: I won't warn you again! – 93irish
  788 2.421405  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife69@2844.com>, subject: Infected your computer! – dcjDik,
  839 2.545584  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife42@9083.com>, subject: I got everything! – 121212,  (tex
  904 2.732556  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife56@7082.com>, subject: Read carefully! – dayrit,  (text/
  948 2.780453  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife91@3903.com>, subject: I can destroy everything! – 12345
  965 2.811168  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife02@7678.com>, subject: Your password! – nafd111,  (text/
  998 2.890149  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife59@3510.com>, subject: Data of you and your family! – pe
 1022 2.951297  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife01@6073.com>, subject: Pay! – 12345,  (text/plain) | .
 1029 2.951974  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife01@6073.com>, subject: Pay! – tomcat,  (text/plain) | .
 1051 2.966874  10.6.1.104  98.137.159.26   SMTP/…     59 from: Your Life<YourLife97@6073.com>, subject: Videos of you! – 122577,  (text/p
 1119 3.076453  10.6.1.104  106.10.248.75   SMTP/…     59 from: Your Life<YourLife53@3510.com>, subject: I seen everything! – xbdmiy4,  (t
```

```
> Frame 338: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interfa
> Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93
> Internet Protocol Version 4, Src: 10.6.1.104, Dst: 98.137.159.26
> Transmission Control Protocol, Src Port: 49181, Dst Port: 25, Seq: 2553, Ack: 2
> Simple Mail Transfer Protocol
v Internet Message Format
    Received: from ffsrjaa ([29.140.42.132]) by 19322.com with MailEnable ESMTP;
    Received: (qmail 19322 invoked by uid 193);
  > From: Your Life<YourLife36@7162.com>, 1 item
  > To: ikwlngpoh@yahoo.com, 1 item
    Subject: Hurry up and pay! – ganjaman
    Date: Sat, 1 Jun 2019 08:35:10 +0000
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ·*····· ··G···E·
0010  00 2d 07 2c 40 00 80 06  e6 8d 0a 06 01 68 62 89   ·-·,@··· ·····hb·
0020  9f 1a c0 1d 00 19 e3 c2  ba cb 97 fb dd d3 50 18   ········ ······P·
0030  fa 08 8f 01 00 00 0d 0a  2e 0d 0a                  ········ .··
```

Stretch Challenge (Optional)

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



YL

Your Life

Hurry up and pay! - ganjaman

To: ikwingpoh@yahoo.com

June 1, 2019 at 1:35 AM

Hi!

I know that: ganjaman - 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

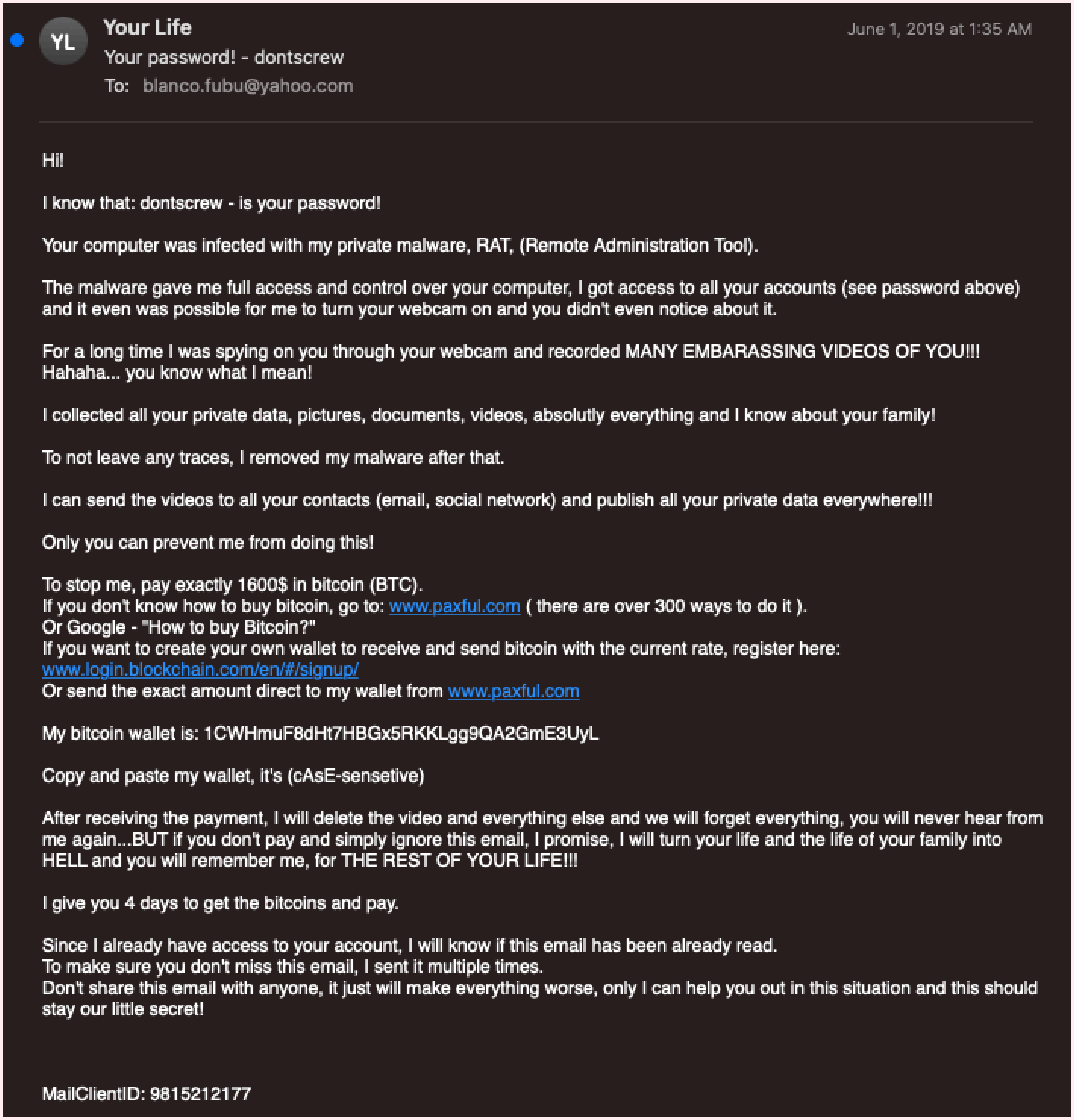
Copy and paste my wallet, it's (cAsE-sensetive)

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: 5972073525



Your Life

Your password! - dontscrew

To: blanco.fubu@yahoo.com

June 1, 2019 at 1:35 AM

Hi!

I know that: dontscrew - 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

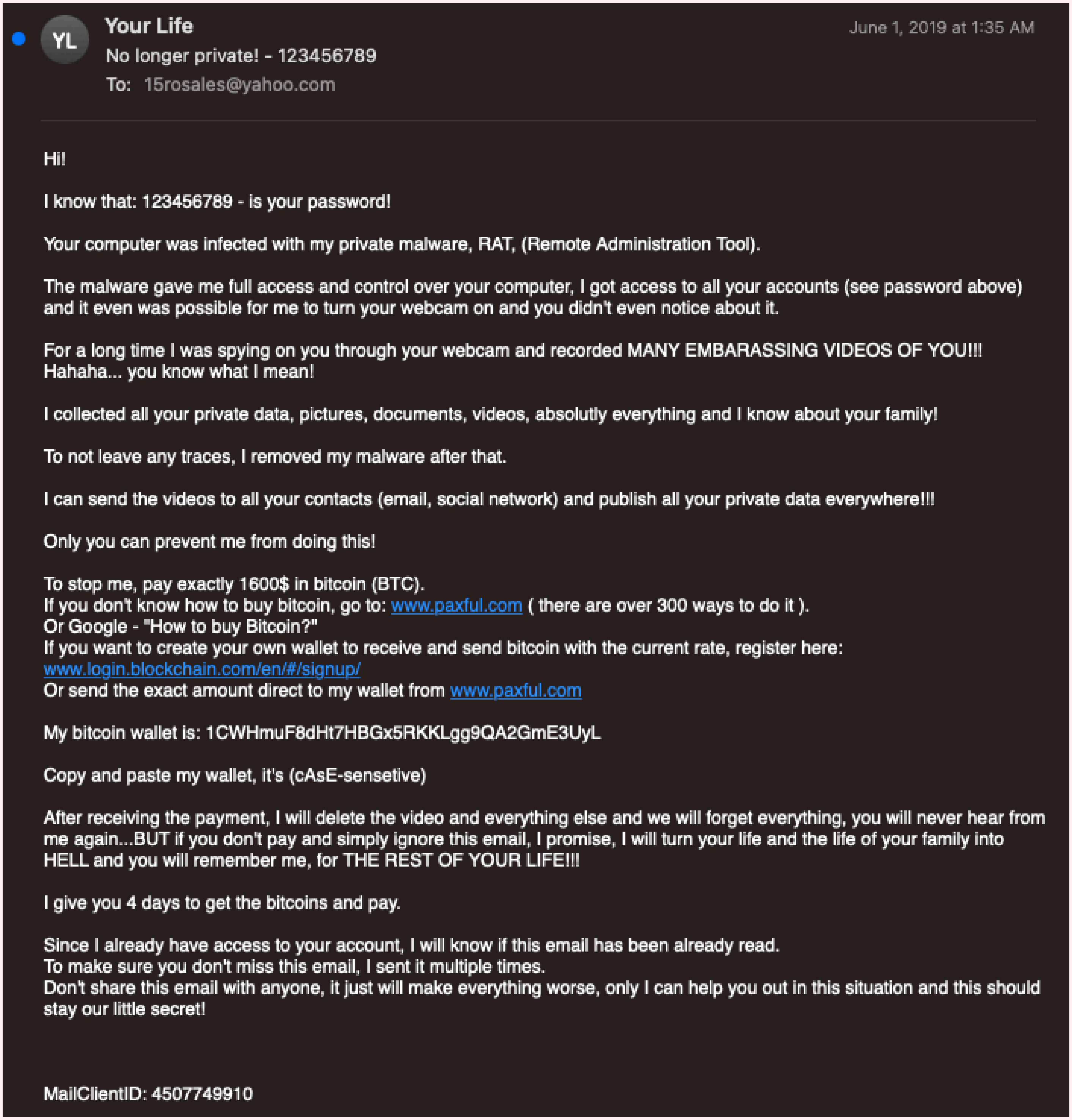
Copy and paste my wallet, it's (cAsE-sensetive)

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: 9815212177



YL

Your Life

No longer private! - 123456789

To: 15rosales@yahoo.com

June 1, 2019 at 1:35 AM

Hi!

I know that: 123456789 - 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: 4507749910

Notes (Optional): After going through the Wireshark capture analysis, I exported three of the objects to IML files. Each IML file shows the content of the phishing email from the malicious actor.

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~~

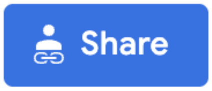
Stretch Challenge

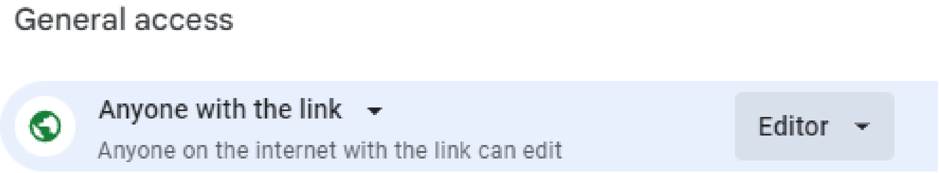
- ☑ ~~Item #1~~

💡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.





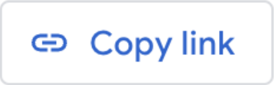
General access

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.