CYB102 Project 1

(🔗 Instructions Page)

👤 Student Name: Alexander Nguyen

✉️ Student Email: alexanderhonguyen19@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!)
>
> 🚩📤📦

> 🧠**Reflection Question #2:** How does Wireshark help us to analyze network traffic?
>
> It certainly helped me find the specific ip address. And using wireshark to sniff that out.
> We can also filter out the and follow the stream, seeing all the emails and the contents sent to each user.

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!
>
> I mostly talked about the analyze > follow > tcp stream, for my teammates.
> I thought it would be helpful for them to look at a specific packet.
> We haven't talked much afterwards though.

Required Challenges (Required)

> **Item #1:** The bad apple's IP address:
>
> **192.168.1.4**
> **217.12.11.66**

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

1. Subject: Hurry up and pay! - ganjaman
2. Subject: Your privacy! - J4k4rt4
3. Subject: I don't play any games! - batman

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!)

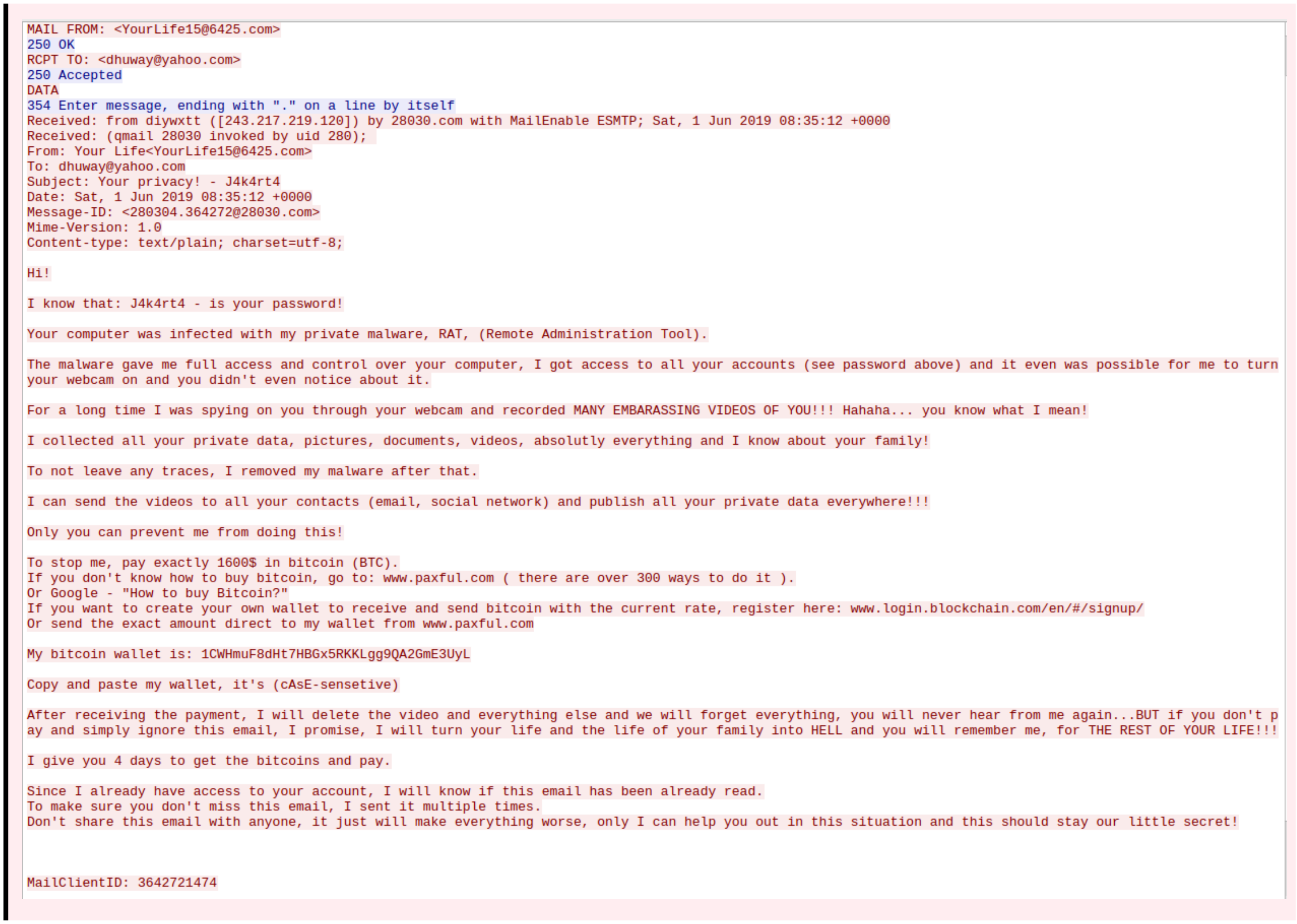
I mostly used the button with › analyze › follow › TCP stream.
Then I look through the emails sent from the bad apple to the phishing victim, and look through the email contents that the bad apple has sent.

There was also a useful filter called "smtp.data.fragment" which I used to find the subject lines for each of the phishing mails. I noticed there were a lot of mails then I realized and it helped me get item #2.
I might be confused with the bad apple's ip address. Is it only the first and fourth pcap files or is it including the ones from the second and third pcap. Or they were using a different pcap entirely. I checked with other tools such as NetworkMiner that the phishing emails that send to the victims were using a remote desktop instead of the original Windows os.

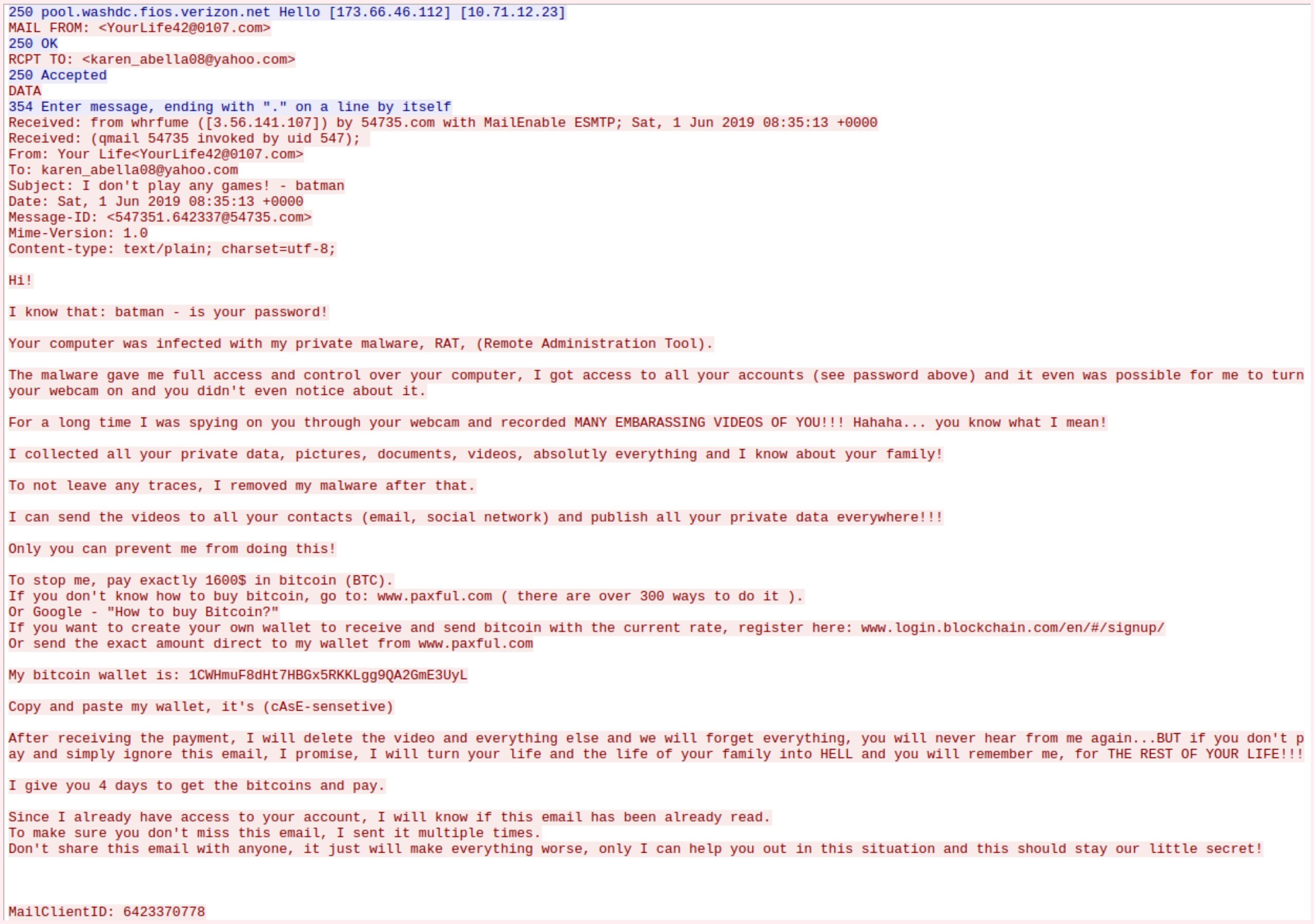
Stretch Challenge (Optional)

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

```
250 pool.washdc.fios.verizon.net Hello [173.66.46.112] [10.71.12.23]
MAIL FROM: <YourLife36@7162.com>
250 OK
RCPT TO: <ikwlngpoh@yahoo.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
Received: from ffsrjaa ([29.140.42.132]) by 19322.com with MailEnable ESMTP; Sat, 1 Jun 2019 08:35:10 +0000
Received: (qmail 19322 invoked by uid 193);
From: Your Life<YourLife36@7162.com>
To: ikwlngpoh@yahoo.com
Subject: Hurry up and pay! - ganjaman
Date: Sat, 1 Jun 2019 08:35:10 +0000
Message-ID: <193221.597207@19322.com>
Mime-Version: 1.0
Content-type: text/plain; charset=utf-8;

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 p
ay 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
```



```
MAIL FROM: <YourLife15@6425.com>
250 OK
RCPT TO: <dhuway@yahoo.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
Received: from diywxtt ([243.217.219.120]) by 28030.com with MailEnable ESMTP; Sat, 1 Jun 2019 08:35:12 +0000
Received: (qmail 28030 invoked by uid 280);
From: Your Life<YourLife15@6425.com>
To: dhuway@yahoo.com
Subject: Your privacy! - J4k4rt4
Date: Sat, 1 Jun 2019 08:35:12 +0000
Message-ID: <280304.364272@28030.com>
Mime-Version: 1.0
Content-type: text/plain; charset=utf-8;

Hi!

I know that: J4k4rt4 - 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 p
ay 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: 3642721474
```



```
250 pool.washdc.fios.verizon.net Hello [173.66.46.112] [10.71.12.23]
MAIL FROM: <YourLife42@0107.com>
250 OK
RCPT TO: <karen_abella08@yahoo.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
Received: from whrfume ([3.56.141.107]) by 54735.com with MailEnable ESMTP; Sat, 1 Jun 2019 08:35:13 +0000
Received: (qmail 54735 invoked by uid 547);
From: Your Life<YourLife42@0107.com>
To: karen_abella08@yahoo.com
Subject: I don't play any games! - batman
Date: Sat, 1 Jun 2019 08:35:13 +0000
Message-ID: <547351.642337@54735.com>
Mime-Version: 1.0
Content-type: text/plain; charset=utf-8;

Hi!

I know that: batman - 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 p
ay 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: 6423370778
```

Notes (Optional):

This was optional, but I was upskilling with Wireshark and asking a discord server for help. Some smarter people helped me learn how to extract the file seemingly. Without the binary parts get fumbled with the ascii code.

"Go to your email tcp stream -> Switch to Raw -> Save as -> change the extension to .eml"
And I checked in HexEd.it to verify I did the extraction of the .eml file with its contents.
Not necessary, but really cool to know about the NetworkMiner tool.

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~~