


CYB102 Project 1


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?

By viewing capture files, we can see the packets of data transmitted through the network, allowing us to view both the metadata and the ASCII contents of each packet.

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

Shoutout to the Assignment Reminder bot in Slack!

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. Read carefully! – dayrit**
- 2. I can destroy everything! – 12345678**
- 3. Data of you and your family! – peace**

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 used “smtp” in the search and started looking at the Info category to see the words “from”

and “subject” as these keywords would help me identify the sent phishing emails.

Stretch Challenge (Optional)

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

```
Received: from jzifcym ([6.15.228.98]) by 67245.com with MailEnable ESMT; Sat, 1 Jun 2019 08:35:11 +0000
Received: (qmail 67245 invoked by uid 672);
From: Your Life<YourLife56@7082.com>
To: loren.khulot@yahoo.com
Subject: Read carefully! - dayrit
Date: Sat, 1 Jun 2019 08:35:11 +0000
Message-ID: <672457.878423@67245.com>
Mime-Version: 1.0
Content-type: text/plain; charset=utf-8;
```

Hi!

I know that: dayrit - 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 EMBARRASSING VIDEOS OF YOU!!! Hahaha... you know what I mean!

I collected all your private data, pictures, documents, videos, absolutely 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: 1CWmhuF8dHt7HBGx5RKKLgg9QA2GmE3UyL

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

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.

```
Received: from axvgrss ([74.8.13.159]) by 04008.com with MailEnable ESMT; Sat, 1 Jun 2019 08:35:11 +0000
Received: (qmail 04008 invoked by uid 040);
From: Your Life<YourLife91@3903.com>
To: mizz_china_01@yahoo.com
Subject: I can destroy everything! - 12345678
Date: Sat, 1 Jun 2019 08:35:11 +0000
Message-ID: <040083.126871@04008.com>
Mime-Version: 1.0
Content-type: text/plain; charset=utf-8;
```

Hi!

I know that: 12345678 - 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 EMBARRASSING VIDEOS OF YOU!!! Hahaha... you know what I mean!

I collected all your private data, pictures, documents, videos, absolutely 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: 1CWmhuF8dHt7HBGx5RKKLgg9QA2GmE3UyL

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

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.

```
Received: from wvpebim ([147.72.115.149]) by 63317.com with MailEnable ESMTP; Sat, 1 Jun 2019 08:35:11 +0000
Received: (qmail 63317 invoked by uid 633);
From: Your Life<YourLife59@3510.com>
To: mr_msnv4_09@yahoo.com
Subject: Data of you and your family! - peace
Date: Sat, 1 Jun 2019 08:35:11 +0000
Message-ID: <633173.719931@63317.com>
Mime-Version: 1.0
Content-type: text/plain; charset=utf-8;
```

Hi|

I know that: peace - 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 EMBARRASSING VIDEOS OF YOU!!! Hahaha... you know what I mean!

I collected all your private data, pictures, documents, videos, absolutely 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.

Notes (Optional):

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.

Grading

Total Score *
14/16 points
88%

Scoring Breakdown

Category	Feature	Evaluation	Expectation	Points Awarded
Required	Reflection Question #1	There is a response provided.	A response must be provided.	2
Required	Reflection Question #2	There is a response provided.	A response must be provided.	2
Required	Rogue user's IP address	The IP address identified is 10.6.1.104.	This IP address should be the source IP address as shown in your results.	4
Required	Subject lines of phishing emails.	There are three phishing subject lines identified.	There must be 3 phishing subject lines provided from your search query.	3
Required	Explanation of finding the rouge user from just the .pcap files	The fraudulent emails are searched using SMTP, SMTP contains "FROM" or other insufficient filters.	The explanation should mention the correct and most appropriate filter used in identifying the fraudulent emails. Check out Wireshark's SMTP reference guide in resources tab in the course portal for the complete list of filters.	0
Stretch	.eml screenshots showing the content of phishing emails	There are three correct screenshots of the content of the .eml files of three different phishing emails.	There should be three screenshots of three different .eml files showing the content of phishing emails.	3